SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 February 2024

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-1709	ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.	10.0	More Details
CVE-2024-1403	In OpenEdge Authentication Gateway and AdminServer prior to 11.7.19, 12.2.14, 12.8.1 on all platforms supported by the OpenEdge product, an authentication bypass vulnerability has been identified. The vulnerability is a bypass to authentication based on a failure to properly handle username and password. Certain unexpected content passed into the credentials can lead to unauthorized access without proper authentication.	10.0	More Details
CVE-2024-25913	Unrestricted Upload of File with Dangerous Type vulnerability in Skymoonlabs MoveTo.This issue affects MoveTo: from n/a through 6.2.	10.0	More Details
CVE-2024-1212	Unauthenticated remote attackers can access the system through the LoadMaster management interface, enabling arbitrary system command execution.	10.0	More Details
CVE-2024-25925	Unrestricted Upload of File with Dangerous Type vulnerability in SYSBASICS WooCommerce Easy Checkout Field Editor, Fees & Discounts.This issue affects WooCommerce Easy Checkout Field Editor, Fees & Discounts: from n/a through 3.5.12.	10.0	More Details
CVE-2024-25909	Unrestricted Upload of File with Dangerous Type vulnerability in JoomUnited WP Media folder.This issue affects WP Media folder: from n/a through 5.7.2.	9.9	More Details
CVE-2023-51389	Hertzbeat is a real-time monitoring system. At the interface of `/define/yml`, SnakeYAML is used as a parser to parse yml content, but no security configuration is used, resulting in a YAML deserialization vulnerability. Version 1.4.1 fixes this vulnerability.	9.8	More Details
CVE-2023-51653	Hertzbeat is a real-time monitoring system. In the implementation of `JmxCollectImpl.java`, `JMXConnectorFactory.connect` is vulnerable to JNDI injection. The corresponding interface is `/api/monitor/detect`. If there is a URL field, the address will be used by default. When the URL is `service:jmx:rmi:///jndi/rmi://xxxxxxx:1099/localHikari`, it can be exploited to cause remote code execution. Version 1.4.1 contains a fix for this issue.	9.8	More Details
CVE-2024-25802	SKINsoft S-Museum 7.02.3 allows Unrestricted File Upload via the Add Media function. Unlike in CVE-2024-25801, the attack payload is the file content.	9.8	More Details
CVE-2024-1783	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130/9.3.5u.6698_B20230810. Affected is the function loginAuth of the file /cgi-bin/cstecgi.cgi of the component Web Interface. The manipulation of the argument http_host leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-254574 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2024-25730	Hitron CODA-4582 and CODA-4589 devices have default PSKs that are generated from 5-digit hex values concatenated with a "Hitron" substring, resulting in insufficient entropy (only about one million possibilities).	9.8	More Details
CVE-2024-22988	An issue in zkteco zkbio WDMS v.8.0.5 allows an attacker to execute arbitrary code via the /files/backup/ component.	9.8	More Details
CVE-2023-49959	In Indo-Sol PROFINET-INspektor NT through 2.4.0, a command injection vulnerability in the gedtupdater service of the firmware allows remote attackers to execute arbitrary system commands with root privileges via a crafted filename parameter in POST requests to the /api/updater/ctrl/start_update endpoint.	9.8	More Details
CVE-2024-27444	langchain_experimental (aka LangChain Experimental) in LangChain before 0.1.8 allows an attacker to bypass the CVE-2023-44467 fix and execute arbitrary code via the __import__, __subclasses__, __builtins__, __globals__, __getattribute__, __bases__, __mro__, or __base__ attribute in Python code. These are not prohibited by pal_chain/base.py.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25850	Netis WF2780 v2.1.40144 was discovered to contain a command injection vulnerability via the wps_ap_ssid5g parameter	9.8	More Details
CVE-2024-27447	pretix before 2024.1.1 mishandles file validation.	9.8	More Details
CVE-2024-24401	SQL Injection vulnerability in Nagios XI 2024R1.01 allows a remote attacker to execute arbitrary code via a crafted payload to the monitoringwizard.php component.	9.8	More Details
CVE-2024-25751	A Stack Based Buffer Overflow vulnerability in Tenda AC9 v.3.0 with firmware version v.15.03.06.42_multi allows a remote attacker to execute arbitrary code via the fromSetSysTime function.	9.8	More Details
CVE-2024-25247	SQL Injection vulnerability in /app/api/controller/Store.php in Niushop B2B2C V5 allows attackers to run arbitrary SQL commands via latitude and longitude parameters.	9.8	More Details
CVE-2023-41506	An arbitrary file upload vulnerability in the Update/Edit Student's Profile Picture function of Student Enrollment In PHP v1.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2024-24095	Code-projects Simple Stock System 1.0 is vulnerable to SQL Injection.	9.8	More Details
CVE-2024-1698	The NotificationX – Best FOMO, Social Proof, WooCommerce Sales Popup & Notification Bar Plugin With Elementor plugin for WordPress is vulnerable to SQL Injection via the 'type' parameter in all versions up to, and including, 2.8.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2023-51518	Apache James prior to version 3.7.5 and 3.8.0 exposes a JMX endpoint on localhost subject to pre-authentication deserialisation of untrusted data. Given a deserialisation gadjet, this could be leveraged as part of an exploit chain that could result in privilege escalation. Note that by default JMX endpoint is only bound locally. We recommend users to: - Upgrade to a non-vulnerable Apache James version - Run Apache James isolated from other processes (docker - dedicated virtual machine) - If possible turn off JMX	9.8	More Details
CVE-2024-25843	In the module "Import/Update Bulk Product from any Csv/Excel File Pro" (ba_importer) up to version 1.1.28 from Buy Addons for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-51388	Hertzbeat is a real-time monitoring system. In `CalculateAlarm.java`, `AviatorEvaluator` is used to directly execute the expression function, and no security policy is configured, resulting in AviatorScript (which can execute any static method by default) script injection. Version 1.4.1 fixes this vulnerability.	9.8	More Details
CVE-2024-27099	The uAMQP is a C library for AMQP 1.0 communication to Azure Cloud Services. When processing an incorrect `AMQP_VALUE` failed state, may cause a double free problem. This may cause a RCE. Update submodule with commit 2ca42b6e4e098af2d17e487814a91d05f6ae4987.	9.8	More Details
CVE-2023-52153	A SQL Injection vulnerability in /pmb/opac_css/includes/sessions.inc.php in PMB 7.4.7 and earlier allows remote unauthenticated attackers to inject arbitrary SQL commands via the PmbOpac-LOGIN cookie value.	9.8	More Details
CVE-2023-51828	A SQL Injection vulnerability in /admin/convert/export.class.php in PMB 7.4.7 and earlier versions allows remote unauthenticated attackers to execute arbitrary SQL commands via the query parameter in get_next_notice function.	9.8	More Details
CVE-2023-37177	SQL Injection vulnerability in PMB Services PMB v.7.4.7 and before allows a remote unauthenticated attacker to execute arbitrary code via the query parameter in the /admin/convert/export_z3950.php endpoint.	9.8	More Details
CVE-2023-24331	Command Injection vulnerability in D-Link Dir 816 with firmware version DIR-816_A2_v1.10CNB04 allows attackers to run arbitrary commands via the urlAdd parameter.	9.8	More Details
CVE-2024-25897	ChurchCRM 5.5.0 FRCatalog.php is vulnerable to Blind SQL Injection (Time-based) via the CurrentFundraiser GET parameter.	9.8	More Details
CVE-2024-25894	ChurchCRM 5.5.0 /EventEditor.php is vulnerable to Blind SQL Injection (Time-based) via the EventCount POST parameter.	9.8	More Details
CVE-2024-25147	Cross-site scripting (XSS) vulnerability in HtmlUtil.escapeJsLink in Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via crafted javascript: style links.	9.6	More Details
CVE-2024-26269	Cross-site scripting (XSS) vulnerability in the Frontend JS module's portlet.js in Liferay Portal 7.2.0 through 7.4.3.37, and Liferay DXP 7.4 before update 38, 7.3 before update 11, 7.2 before fix pack 20, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via the anchor (hash) part of a URL.	9.6	More Details
CVE-2023-42496	Reflected cross-site scripting (XSS) vulnerability on the add assignees to a role page in Liferay Portal 7.3.3 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 6, 7.4 GA through update 92, and 7.3 before update 34 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_roles_admin_web_portlet_RolesAdminPortlet_tabs2 parameter.	9.6	More Details
CVE-2023-42498	Reflected cross-site scripting (XSS) vulnerability in the Language Override edit screen in Liferay Portal 7.4.3.8 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 5, and 7.4 update 4 through 92 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portal_language_override_web_internal_portlet_PLOPortlet_key parameter.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25124	Fiber is a web framework written in go. Prior to version 2.52.1, the CORS middleware allows for insecure configurations that could potentially expose the application to multiple CORS-related vulnerabilities. Specifically, it allows setting the Access-Control-Allow-Origin header to a wildcard (`*`) while also having the Access-Control-Allow-Credentials set to true, which goes against recommended security best practices. The impact of this misconfiguration is high as it can lead to unauthorized access to sensitive user data and expose the system to various types of attacks listed in the PortSwigger article linked in the references. Version 2.52.1 contains a patch for this issue. As a workaround, users may manually validate the CORS configurations in their implementation to ensure that they do not allow a wildcard origin when credentials are enabled. The browser fetch api, as well as browsers and utilities that enforce CORS policies, are not affected by this.	9.4	More Details
CVE-2024-23346	Pymatgen (Python Materials Genomics) is an open-source Python library for materials analysis. A critical security vulnerability exists in the `JonesFaithfulTransformation.from_transformation_str()` method within the `pymatgen` library prior to version 2024.2.20. This method insecurely utilizes `eval()` for processing input, enabling execution of arbitrary code when parsing untrusted input. Version 2024.2.20 fixes this issue.	9.3	More Details
CVE-2024-25846	In the module "Product Catalog (CSV, Excel) Import" (simpleimportproduct) <= 6.7.0 from MyPrestaModules for PrestaShop, a guest can upload files with extensions .php.	9.1	More Details
CVE-2024-27905	** UNSUPPORTED WHEN ASSIGNED ** Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Aurora. An endpoint exposing internals to unauthenticated users can be used as a "padding oracle" allowing an anonymous attacker to construct a valid authentication cookie. Potentially this could be combined with vulnerabilities in other components to achieve remote code execution. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.1	More Details
CVE-2024-1631	Impact: The library offers a function to generate an ed25519 key pair via Ed25519KeyIdentity.generate with an optional param to provide a 32 byte seed value, which will then be used as the secret key. When no seed value is provided, it is expected that the library generates the secret key using secure randomness. However, a recent change broke this guarantee and uses an insecure seed for key pair generation. Since the private key of this identity (535yc-uxytb-gfk7h-tny7p-vjkoe-i4krp-3qmcl-uqfgr-cpgej-yqtjq-rqe) is compromised, one could lose funds associated with the principal on ledgers or lose access to a canister where this principal is the controller.	9.1	More Details
CVE-2024-22393	Unrestricted Upload of File with Dangerous Type vulnerability in Apache Answer.This issue affects Apache Answer: through 1.2.1. Pixel Flood Attack by uploading large pixel files will cause server out of memory. A logged-in user can cause such an attack by uploading an image when posting content. Users are recommended to upgrade to version [1.2.5], which fixes the issue.	9.1	More Details
CVE-2024-27456	rack-cors (aka Rack CORS Middleware) 2.0.1 has 0666 permissions for the .rb files.	9.1	More Details
CVE-2024-25893	ChurchCRM 5.5.0 FRCertificates.php is vulnerable to Blind SQL Injection (Time-based) via the CurrentFundraiser GET parameter.	9.1	More Details
CVE-2024-1735	A vulnerability has been identified in armeria-saml versions less than 1.27.2, allowing the use of malicious SAML messages to bypass authentication. All users who rely on armeria-saml older than version 1.27.2 must upgrade to 1.27.2 or later.	9.1	More Details
CVE-2024-27455	In the Bentley ALIM Web application, certain configuration settings can cause exposure of a user's ALIM session token when the user attempts to download files. This is fixed in Assetwise ALIM Web 23.00.04.04 and Assetwise Information Integrity Server 23.00.02.03.	9.1	More Details
CVE-2024-26266	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.2.0 through 7.4.3.13, and older unsupported versions, and Liferay DXP 7.4 before update 10, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allow remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into the first/middle/last name text field of the user who creates an entry in the (1) Announcement widget, or (2) Alerts widget.	9.0	More Details
CVE-2024-25603	Stored cross-site scripting (XSS) vulnerability in the Dynamic Data Mapping module's DDMForm in Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via the instanceId parameter.	9.0	More Details
CVE-2024-25152	Stored cross-site scripting (XSS) vulnerability in Message Board widget in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via the filename of an attachment.	9.0	More Details
CVE-2023-47795	Stored cross-site scripting (XSS) vulnerability in the Document and Media widget in Liferay Portal 7.4.3.18 through 7.4.3.101, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 18 through 92 allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a document's “Title” text field.	9.0	More Details
CVE-2023-46241	`discourse-microsoft-auth` is a plugin that enables authentication via Microsoft. On sites with the `discourse-microsoft-auth` plugin enabled, an attack can potentially take control of a victim's Discourse account. Sites that have configured their application's account type to any options other than `Accounts in this organizational directory only (O365 only - Single tenant)` are vulnerable. This vulnerability has been patched in commit c40665f44509724b64938c85def9fb2e79f62ec8 of `discourse-microsoft-auth`. A `microsoft_auth:revoke` rake task has also been added which will deactivate and log out all users that have connected their accounts to Microsoft. User API keys as well as API keys created by those users will also be revoked. The rake task will also remove the connection records to Microsoft for those users. This will allow affected users to re-verify their account emails as well as reconnect their Discourse account to Microsoft for authentication. As a workaround, disable the `discourse-microsoft-auth` plugin by setting the `microsoft_auth_enabled` site setting to `false`. Run the `microsoft_auth:log_out_users` rake task to log out all users with associated Microsoft accounts.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40191	Reflected cross-site scripting (XSS) vulnerability in the instance settings for Accounts in Liferay Portal 7.4.3.44 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 44 through 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into the “Blocked Email Domains” text field	9.0	More Details
CVE-2024-25602	Stored cross-site scripting (XSS) vulnerability in Users Admin module's edit user page in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into an organization’s “Name” text field	9.0	More Details
CVE-2024-25601	Stored cross-site scripting (XSS) vulnerability in Expando module's geolocation custom fields in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into the name text field of a geolocation custom field.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Re
CVE-2024-26352	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/add_places.php	8.8	Mo De
CVE-2023-29181	A use of externally-controlled format string in Fortinet FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiPAM 1.0.0 through 1.0.3 allows attacker to execute unauthorized code or commands via specially crafted command.	8.8	Mo De
CVE-2023-50379	Malicious code injection in Apache Ambari in prior to 2.7.8. Users are recommended to upgrade to version 2.7.8, which fixes this issue. Impact: A Cluster Operator can manipulate the request by adding a malicious code injection and gain a root over the cluster main host.	8.8	Mo De
CVE-2023-24330	Command Injection vulnerability in D-Link Dir 882 with firmware version DIR882A1_FW130B06 allows attackers to run arbitrary commands via crafted POST request to /HNAP1/.	8.8	Mo De
CVE-2024-25251	code-projects Agro-School Management System 1.0 is suffers from Incorrect Access Control.	8.8	Mo De
CVE-2024-21836	A heap-based buffer overflow vulnerability exists in the GGUF library header.n_tensors functionality of llama.cpp Commit 18c2e17. A specially crafted .gguf file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	Mo De
CVE-2024-21825	A heap-based buffer overflow vulnerability exists in the GGUF library GGUF_TYPE_ARRAY/GGUF_TYPE_STRING parsing functionality of llama.cpp Commit 18c2e17. A specially crafted .gguf file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	Mo De
CVE-2024-25746	Stack Based Buffer Overflow vulnerability in Tenda AC9 v.3.0 with firmware version v.15.03.06.42_multi allows a remote attacker to execute arbitrary code via the add_white_node function.	8.8	Mo De
CVE-2024-26483	An arbitrary file upload vulnerability in the Profile Image module of Kirby CMS v4.1.0 allows attackers to execute arbitrary code via a crafted PDF file.	8.8	Mo De
CVE-2024-21802	A heap-based buffer overflow vulnerability exists in the GGUF library info->ne functionality of llama.cpp Commit 18c2e17. A specially crafted .gguf file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	Mo De
CVE-2024-1889	Cross-Site Request Forgery vulnerability in SMA Cluster Controller, affecting version 01.05.01.R. This vulnerability could allow an attacker to send a malicious link to an authenticated user to perform actions with these user permissions on the affected device.	8.8	Mo De
CVE-2024-25748	A Stack Based Buffer Overflow vulnerability in tenda AC9 AC9 v.3.0 with firmware version v.15.03.06.42_multi allows a remote attacker to execute arbitrary code via the fromSetIpMacBind function.	8.8	Mo De
CVE-2024-25753	Stack Based Buffer Overflow vulnerability in Tenda AC9 v.3.0 with firmware version v.15.03.06.42_multi allows a remote attacker to execute arbitrary code via the formSetDeviceName function.	8.8	Mo De
CVE-2023-36237	Cross Site Request Forgery vulnerability in Bagisto before v.1.5.1 allows an attacker to execute arbitrary code via a crafted HTML script.	8.8	Mo De

CVE Number	Description	Base Score	Re
CVE-2023-24333	A stack overflow vulnerability in Tenda AC21 with firmware version US_AC21V1.0re_V16.03.08.15_cn_TDC01 allows attackers to run arbitrary commands via crafted POST request to /goform/openSchedWifi.	8.8	Mo De
CVE-2024-1675	Insufficient policy enforcement in Download in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Medium)	8.8	Mo De
CVE-2024-1674	Inappropriate implementation in Navigation in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	8.8	Mo De
CVE-2024-1673	Use after free in Accessibility in Google Chrome prior to 122.0.6261.57 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	8.8	Mo De
CVE-2024-1710	The Addon Library plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the onAjaxAction function action in all versions up to, and including, 1.3.76. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform several unauthorized actions including uploading arbitrary files.	8.8	Mo De
CVE-2024-23496	A heap-based buffer overflow vulnerability exists in the GGUF library gguf_fread_str functionality of llama.cpp Commit 18c2e17. A specially crafted .gguf file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	Mo De
CVE-2024-1670	Use after free in Mojo in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	Mo De
CVE-2024-1669	Out of bounds memory access in Blink in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	Mo De
CVE-2024-23605	A heap-based buffer overflow vulnerability exists in the GGUF library header.n_kv functionality of llama.cpp Commit 18c2e17. A specially crafted .gguf file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	Mo De
CVE-2024-24310	In the module "Generate barcode on invoice / delivery slip" (ecgeneratebarcode) from Ether Creation <= 1.2.0 for PrestaShop, a guest can perform SQL injection.	8.8	Mo De
CVE-2024-23320	Improper Input Validation vulnerability in Apache DolphinScheduler. An authenticated user can cause arbitrary, unsandboxed javascript to be executed on the server. This issue is a legacy of CVE-2023-49299. We didn't fix it completely in CVE-2023-49299, and we added one more patch to fix it. This issue affects Apache DolphinScheduler: until 3.2.1. Users are recommended to upgrade to version 3.2.1, which fixes the issue.	8.8	Mo De
CVE-2024-23094	Flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /cover/addons/info_media_gallery/action/edit_addon_post.php	8.8	Mo De
CVE-2024-25723	ZenML Server in the ZenML machine learning package before 0.46.7 for Python allows remote privilege escalation because the /api/v1/users/{user_name_or_id}/activate REST API endpoint allows access on the basis of a valid username along with a new password in the request body. These are also patched versions: 0.44.4, 0.43.1, and 0.42.2.	8.8	Mo De
CVE-2024-1451	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.9 before 16.9.1. A crafted payload added to the user profile page could lead to a stored XSS on the client side, allowing attackers to perform arbitrary actions on behalf of victims."	8.7	Mo De
CVE-2024-26150	`@backstage/backend-common` is a common functionality library for backends for Backstage, an open platform for building developer portals. In `@backstage/backend-common` prior to versions 0.21.1, 0.20.2, and 0.19.10, paths checks with the `resolveSafeChildPath` utility were not exhaustive enough, leading to risk of path traversal vulnerabilities if symlinks can be injected by attackers. This issue is patched in `@backstage/backend-common` versions 0.21.1, 0.20.2, and 0.19.10.	8.7	Mo De
CVE-2023-42838	An access issue was addressed with improvements to the sandbox. This issue is fixed in macOS Ventura 13.6.3, macOS Sonoma 14.1, macOS Monterey 12.7.2. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	8.6	Mo De
CVE-2024-22917	SQL injection vulnerability in Dynamic Lab Management System Project in PHP v.1.0 allows a remote attacker to execute arbitrary code via a crafted script.	8.6	Mo De
CVE-2021-33141	Improper input validation in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow an unauthenticated user to potentially enable denial of service via network access.	8.6	Mo De
CVE-2022-43842	IBM Aspera Console 3.4.0 through 3.4.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 239079.	8.6	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-33162	Improper access control in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow an authenticated user to potentially enable escalation of privilege via local access.	8.4	Mo De
CVE-2023-7235	The OpenVPN GUI installer before version 2.6.9 did not set the proper access control restrictions to the installation directory of OpenVPN binaries when using a non-standard installation path, which allows an attacker to replace binaries to run arbitrary executables.	8.4	Mo De
CVE-2024-25021	IBM AIX 7.3, VIOS 4.1's Perl implementation could allow a non-privileged local user to exploit a vulnerability to execute arbitrary commands. IBM X-Force ID: 281320.	8.4	Mo De
CVE-2024-1708	ConnectWise ScreenConnect 23.9.7 and prior are affected by path-traversal vulnerability, which may allow an attacker the ability to execute remote code or directly impact confidential data or critical systems.	8.4	Mo De
CVE-2023-50975	The TD Bank TD Advanced Dashboard client through 3.0.3 for macOS allows arbitrary code execution because of the lack of electron::fuses::IsRunAsNodeEnabled (i.e., ELECTRON_RUN_AS_NODE can be used in production). This makes it easier for a compromised process to access banking information.	8.4	Mo De
CVE-2021-46973	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: Avoid potential use after free in MHI send It is possible that the MHI ul_callback will be invoked immediately following the queueing of the skb for transmission, leading to the callback decrementing the refcount of the associated sk and freeing the skb. As such the dereference of skb and the increment of the sk refcount must happen before the skb is queued, to avoid the skb to be used after free and potentially the sk to drop its last refcount..	8.4	Mo De
CVE-2024-0220	B&R Automation Studio Upgrade Service and B&R Technology Guarding use insufficient cryptography for communication to the upgrade and the licensing servers. A network-based attacker could exploit the vulnerability to execute arbitrary code on the products or sniff sensitive data.	8.3	Mo De
CVE-2024-26151	The `mjml` PyPI package, found at the `FelixSchwarz/mjml-python` GitHub repo, is an unofficial Python port of MJML, a markup language created by Mailjet. All users of `FelixSchwarz/mjml-python` who insert untrusted data into mjml templates unless that data is checked in a very strict manner. User input like `&lt;script&gt;` would be rendered as `<script>` in the final HTML output. The attacker must be able to control some data which is later injected in an mjml template which is then send out as email to other users. The attacker could control contents of email messages sent through the platform. The problem has been fixed in version 0.11.0 of this library. Versions before 0.10.0 are not affected by this security issue. As a workaround, ensure that potentially untrusted user input does not contain any sequences which could be rendered as HTML.	8.2	Mo De
CVE-2024-26192	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	8.2	Mo De
CVE-2024-25892	ChurchCRM 5.5.0 ConfirmReport.php is vulnerable to Blind SQL Injection (Time-based) via the familyId GET parameter.	8.1	Mo De
CVE-2024-22243	Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks.	8.1	Mo De
CVE-2024-22873	Tencent Blueking CMDB v3.2.x to v3.9.x was discovered to contain a Server-Side Request Forgery (SSRF) via the event subscription function (/service/subscription.go). This vulnerability allows attackers to access internal requests via a crafted POST request.	8.1	Mo De
CVE-2023-24332	A stack overflow vulnerability in Tenda AC6 with firmware version US_AC6V5.0re_V03.03.02.01_cn_TDC01 allows attackers to run arbitrary commands via crafted POST request to /goform/PowerSaveSet.	8.1	Mo De
CVE-2024-25756	A Stack Based Buffer Overflow vulnerability in Tenda AC9 v.3.0 with firmware version v.15.03.06.42_multi allows a remote attacker to execute arbitrary code via the formWifiBasicSet function.	8.0	Mo De
CVE-2024-25851	Netis WF2780 v2.1.40144 was discovered to contain a command injection vulnerability via the config_sequence parameter in other_para of cgitest.cgi.	8.0	Mo De
CVE-2023-24334	A stack overflow vulnerability in Tenda AC23 with firmware version US_AC23V1.0re_V16.03.07.45_cn_TDC01 allows attackers to run arbitrary commands via schedStartTime parameter.	8.0	Mo De
CVE-2024-22544	An issue was discovered in Linksys Router E1700 version 1.0.04 (build 3), allows authenticated attackers to execute arbitrary code via the setDateTime function.	8.0	Mo De
CVE-2023-52440	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slub overflow in ksmbd_decode_ntlmssp_auth_blob() If authblob->SessionKey.Length is bigger than session key size(CIFS_KEY_SIZE), slub overflow can happen in key exchange codes. cifs_arc4_crypt copy to session key array from SessionKey from client.	7.8	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46938	In the Linux kernel, the following vulnerability has been resolved: dm rq: fix double free of blk_mq_tag_set in dev remove after table load fails When loading a device-mapper table for a request-based mapped device, and the allocation/initialization of the blk_mq_tag_set for the device fails, a following device remove will cause a double free. E.g. (dmesg): device-mapper: core: Cannot initialize queue for request-based dm-mq mapped device device-mapper: ioctl: unable to set up device queue for new table. Unable to handle kernel pointer dereference in virtual kernel address space Failing address: 0305e098835de000 TEID: 0305e098835de803 Fault in home space mode while using kernel ASCE. AS:000000025efe0007 R3:0000000000000024 Oops: 0038 ilc:3 [#1] SMP Modules linked in: ... lots of modules ... Supported: Yes, External CPU: 0 PID: 7348 Comm: multipathd Kdump: loaded Tainted: G W X 5.3.18-53-default #1 SLE15-SP3 Hardware name: IBM 8561 T01 7I2 (LPAR) Krnl PSW : 0704e00180000000 000000025e368eca (kfree+0x42/0x330) R:0 T:1 IO:1 EX:1 Key:0 M:1 W:0 P:0 AS:3 CC:2 PM:0 RI:0 EA:3 Krnl GPRS: 000000000000004a 000000025efe5230 c1773200d779968d 0000000000000000 000000025e520270 000000025e8d1b40 0000000000000003 00000007aae10000 000000025e5202a2 0000000000000001 c1773200d779968d 0305e098835de640 00000007a8170000 000003ff80138650 000000025e5202a2 000003e00396faa8 Krnl Code: 000000025e368eb8: c4180041e100 lgrl %r1,25eba50b8 000000025e368ebe: ecba06b93a55 risbg %r11,%r10,6,185,58 #000000025e368ec4: e3b010000008 ag %r11,0(%r1) >000000025e368eca: e310b0080004 lg %r1,8(%r11) 000000025e368ed0: a7110001 tmll %r1,1 000000025e368ed4: a7740129 brc 7,25e369126 000000025e368ed8: e320b0080004 lg %r2,8(%r11) 000000025e368ede: b904001b lgr %r1,%r11 Call Trace: [<000000025e368eca>] kfree+0x42/0x330 [<000000025e5202a2>] blk_mq_free_tag_set+0x72/0xb8 [<000003ff801316a8>] dm_mq_cleanup_mapped_device+0x38/0x50 [dm_mod] [<000003ff80120082>] free_dev+0x52/0xd0 [dm_mod] [<000003ff801233f0>] __dm_destroy+0x150/0x1d0 [dm_mod] [<000003ff8012bb9a>] dev_remove+0x162/0x1c0 [dm_mod] [<000003ff8012a988>] ctl_ioctl+0x198/0x478 [dm_mod] [<000003ff8012ac8a>] dm_ctl_ioctl+0x22/0x38 [dm_mod] [<000000025e3b11ee>] ksys_ioctl+0xbe/0xe0 [<000000025e3b127a>] __s390x_sys_ioctl+0x2a/0x40 [<000000025e8c15ac>] system_call+0xd8/0x2c8 Last Breaking-Event-Address: [<000000025e52029c>] blk_mq_free_tag_set+0x6c/0xb8 Kernel panic - not syncing: Fatal exception: panic_on_oops When allocation/initialization of the blk_mq_tag_set fails in dm_mq_init_request_queue(), it is uninitialized/freed, but the pointer is not reset to NULL; so when dev_remove() later gets into dm_mq_cleanup_mapped_device() it sees the pointer and tries to uninitialize and free it again. Fix this by setting the pointer to NULL in dm_mq_init_request_queue() error-handling. Also set it to NULL in dm_mq_cleanup_mapped_device().	7.8	Mo De
CVE-2023-42942	This issue was addressed with improved handling of symlinks. This issue is fixed in watchOS 10.1, macOS Sonoma 14.1, tvOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, macOS Ventura 13.6.1. A malicious app may be able to gain root privileges.	7.8	Mo De
CVE-2023-42928	The issue was addressed with improved bounds checks. This issue is fixed in iOS 17.1 and iPadOS 17.1. An app may be able to gain elevated privileges.	7.8	Mo De
CVE-2023-52469	In the Linux kernel, the following vulnerability has been resolved: drivers/amd/pm: fix a use-after-free in kv_parse_power_table When ps allocated by kzalloc equals to NULL, kv_parse_power_table frees adev->pm.dpm.ps that allocated before. However, after the control flow goes through the following call chains: kv_parse_power_table l-> kv_dpm_init l-> kv_dpm_sw_init l-> kv_dpm_fini The adev->pm.dpm.ps is used in the for loop of kv_dpm_fini after its first free in kv_parse_power_table and causes a use-after-free bug.	7.8	Mo De
CVE-2023-42873	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.1, tvOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	Mo De
CVE-2023-52441	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out of bounds in init_smb2_rsp_hdr() If client send smb2 negotiate request and then send smb1 negotiate request, init_smb2_rsp_hdr is called for smb1 negotiate request since need_neg is set to false. This patch ignore smb1 packets after ->need_neg is set to false.	7.8	Mo De
CVE-2023-52474	In the Linux kernel, the following vulnerability has been resolved: IB/hfi1: Fix bugs with non-PAGE_SIZE-end multi-iovec user SDMA requests hfi1 user SDMA request processing has two bugs that can cause data corruption for user SDMA requests that have multiple payload iovecs where an iovec other than the tail iovec does not run up to the page boundary for the buffer pointed to by that iovec.a Here are the specific bugs: 1. user_sdma_txadd() does not use struct user_sdma_iovec->iov.iov_len. Rather, user_sdma_txadd() will add up to PAGE_SIZE bytes from iovec to the packet, even if some of those bytes are past iovec->iov.iov_len and are thus not intended to be in the packet. 2. user_sdma_txadd() and user_sdma_send_pkts() fail to advance to the next iovec in user_sdma_request->iovs when the current iovec is not PAGE_SIZE and does not contain enough data to complete the packet. The transmitted packet will contain the wrong data from the iovec pages. This has not been an issue with SDMA packets from hfi1 Verbs or PSM2 because they only produce iovecs that end short of PAGE_SIZE as the tail iovec of an SDMA request. Fixing these bugs exposes other bugs with the SDMA pin cache (struct mmu_rb_handler) that get in way of supporting user SDMA requests with multiple payload iovecs whose buffers do not end at PAGE_SIZE. So this commit fixes those issues as well. Here are the mmu_rb_handler bugs that non-PAGE_SIZE-end multi-iovec payload user SDMA requests can hit: 1. Overlapping memory ranges in mmu_rb_handler will result in duplicate pinnings. 2. When extending an existing mmu_rb_handler entry (struct mmu_rb_node), the mmu_rb code (1) removes the existing entry under a lock, (2) releases that lock, pins the new pages, (3) then reacquires the lock to insert the extended mmu_rb_node. If someone else comes in and inserts an overlapping entry between (2) and (3), insert in (3) will fail. The failure path code in this case unpins _all_ pages in either the original mmu_rb_node or the new mmu_rb_node that was inserted between (2) and (3). 3. In hfi1_mmu_rb_remove_unless_exact(), mmu_rb_node->refcount is incremented outside of mmu_rb_handler->lock. As a result, mmu_rb_node could be evicted by another thread that gets mmu_rb_handler->lock and checks mmu_rb_node->refcount before mmu_rb_node->refcount is incremented. 4. Related to #2 above, SDMA request submission failure path does not check mmu_rb_node->refcount before freeing mmu_rb_node object. If there are other SDMA requests in progress whose iovecs have pointers to the now-freed mmu_rb_node(s), those pointers to the now-freed mmu_rb nodes will be dereferenced when those SDMA requests complete.	7.8	Mo De
CVE-2021-46943	In the Linux kernel, the following vulnerability has been resolved: media: staging/intel-ipu3: Fix set_fmt error handling If there in an error during a set_fmt, do not overwrite the previous sizes with the invalid config. Without this patch, v4l2-compliance ends up allocating 4GiB of RAM and causing the following OOPs [38.662975] ipu3-imgu 0000:00:05.0: swiotlb buffer is full (sz: 4096 bytes) [38.662980] DMA: Out of SW-IOMMU space for 4096 bytes at device 0000:00:05.0 [38.663010] general protection fault: 0000 [#1] PREEMPT SMP	7.8	Mo De
CVE-2024-26592	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix UAF issue in ksmbd_tcp_new_connection() The race is between the handling of a new TCP connection and its disconnection. It leads to UAF on `struct tcp_transport` in ksmbd_tcp_new_connection() function.	7.8	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26589	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject variable offset alu on PTR_TO_FLOW_KEYS For PTR_TO_FLOW_KEYS, check_flow_keys_access() only uses fixed off for validation. However, variable offset ptr alu is not prohibited for this ptr kind. So the variable offset is not checked. The following prog is accepted: func#0 @0 0: R1=ctx() R10=fp0 0: (bf) r6 = r1 ; R1=ctx() R6_w=ctx() 1: (79) r7 = *(u64 *)(r6 +144) ; R6_w=ctx() R7_w=flow_keys() 2: (b7) r8 = 1024 ; R8_w=1024 3: (37) r8 /= 1 ; R8_w=scalar() 4: (57) r8 &= 1024 ; R8_w=scalar(smin=smin32=0, smax=umax=smax32=umax32=1024,var_off=(0x0; 0x400)) 5: (0f) r7 += r8 mark_precise: frame0: last_idx 5 first_idx 0 subseq_idx -1 mark_precise: frame0: regs=r8 stack= before 4: (57) r8 &= 1024 mark_precise: frame0: regs=r8 stack= before 3: (37) r8 /= 1 mark_precise: frame0: regs=r8 stack= before 2: (b7) r8 = 1024 6: R7_w=flow_keys(smin=smin32=0,smax=umax=smax32=umax32=1024,var_off =(0x0; 0x400)) R8_w=scalar(smin=smin32=0,smax=umax=smax32=umax32=1024, var_off=(0x0; 0x400)) 6: (79) r0 = *(u64 *)(r7 +0) ; R0_w=scalar() 7: (95) exit This prog loads flow_keys to r7, and adds the variable offset r8 to r7, and finally causes out-of-bounds access: BUG: unable to handle page fault for address: ffffc90014c80038 [...] Call Trace: <TASK> bpf_dispatcher_nop_func include/linux/bpf.h:1231 [inline] __bpf_prog_run include/linux/filter.h:651 [inline] bpf_prog_run include/linux/filter.h:658 [inline] bpf_prog_run_pin_on_cpu include/linux/filter.h:675 [inline] bpf_flow_dissect+0x15f/0x350 net/core/flow_dissector.c:991 bpf_prog_test_run_flow_dissector+0x39d/0x620 net/bpf/test_run.c:1359 bpf_prog_test_run kernel/bpf/syscall.c:4107 [inline] __sys_bpf+0xf8f/0x4560 kernel/bpf/syscall.c:5475 __do_sys_bpf kernel/bpf/syscall.c:5561 [inline] __se_sys_bpf kernel/bpf/syscall.c:5559 [inline] __x64_sys_bpf+0x73/0xb0 kernel/bpf/syscall.c:5559 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x3f/0x110 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Fix this by rejecting ptr alu with variable offset on flow_keys. Applying the patch rejects the program with "R7 pointer arithmetic on flow_keys prohibited".	7.8	Mc De
CVE-2023-42848	The issue was addressed with improved bounds checks. This issue is fixed in watchOS 10.1, macOS Sonoma 14.1, tvOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, macOS Ventura 13.6.1. Processing a maliciously crafted image may lead to heap corruption.	7.8	Mc De
CVE-2024-26588	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Prevent out-of-bounds memory access The test_tag test triggers an unhandled page fault: # ./test_tag [130.640218] CPU 0 Unable to handle kernel paging request at virtual address ffff80001b898004, era == 9000000003137f7c, ra == 9000000003139e70 [130.640501] Oops[#3]: [130.640553] CPU: 0 PID: 1326 Comm: test_tag Tainted: G D O 6.7.0-rc4-loong-devel-gb62ab1a397cf #47 61985c1d94084daa2432f771daa45b56b10d8d2a [130.640764] Hardware name: QEMU QEMU Virtual Machine, BIOS unknown 2/2/2022 [130.640874] pc 9000000003137f7c ra 9000000003139e70 tp 9000000104cb4000 sp 9000000104cb7a40 [130.641001] a0 ffff80001b894000 a1 ffff80001b897ff8 a2 000000006ba210be a3 0000000000000000 [130.641128] a4 000000006ba210be a5 00000000000000f1 a6 0000000000000b3 a7 0000000000000000 [130.641256] t0 0000000000000000 t1 00000000000007f6 t2 0000000000000000 t3 9000000004091b70 [130.641387] t4 000000006ba210be t5 0000000000000004 t6 fffffffffffffff0 t7 90000000040913e0 [130.641512] t8 0000000000000005 u0 00000000000000dc0 s9 0000000000000009 s0 9000000104cb7ae0 [130.641641] s1 00000000000007f6 s2 0000000000000009 s3 0000000000000095 s4 0000000000000000 [130.641771] s5 ffff80001b894000 s6 ffff80001b897fb0 s7 9000000004090c50 s8 0000000000000000 [130.641900] ra: 9000000003139e70 build_body+0x1fcc/0x4988 [130.642007] ERA: 9000000003137f7c build_body+0xd8/0x4988 [130.642112] CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DACM=CC -WE) [130.642261] PRMD: 00000004 (PPLV0 +PIE -PWE) [130.642353] EUEN: 00000003 (+FPE +SXE -ASXE -BTE) [130.642458] ECFG: 00071c1c (LIE=2-4,10-12 VS=7) [130.642554] ESTAT: 00010000 [PIL] (IS= ECode=1 EsubCode=0) [130.642658] BADV: ffff80001b898004 [130.642719] PRID: 0014c010 (Loongson-64bit, Loongson-3A5000) [130.642815] Modules linked in: [last unloaded: bpf_testmod(O)] [130.642924] Process test_tag (pid: 1326, threadinfo=00000000f7f4015f, task=000000006499f9fd) [130.643062] Stack : 0000000000000000 9000000003380724 0000000000000000 0000000104cb7be8 [130.643213] 0000000000000000 25af8d9b6e600558 9000000106250ea0 9000000104cb7ae0 [130.643378] 0000000000000000 0000000000000000 9000000104cb7be8 90000000049f6000 [130.643538] 0000000000000090 9000000106250ea0 ffff80001b894000 ffff80001b894000 [130.643685] 00007ffffb917790 9000000000313ca94 0000000000000000 0000000000000000 [130.643831] ffff80001b894000 0000000000000ff7 0000000000000000 9000000100468000 [130.643983] 0000000000000000 0000000000000000 0000000000000040 25af8d9b6e600558 [130.644131] 0000000000000bb7 ffff80001b894048 0000000000000000 0000000000000000 [130.644276] 9000000104cb7be8 90000000049f6000 0000000000000090 9000000104cb7bdc [130.644423] ffff80001b894000 0000000000000000 00007ffffb917790 90000000032acfb0 [130.644572] ... [130.644629] Call Trace: [130.644641] [<9000000003137f7c>] build_body+0xd8/0x4988 [130.644785] [<9000000003ca94>] bpf_int_jit_compile+0x228/0x4ec [130.644891] [<90000000032acfb0>] bpf_prog_select_runtime+0x158/0x1b0 [130.645003] [<90000000032b3504>] bpf_prog_load+0x760/0xb44 [130.645089] [<90000000032b6744>] __sys_bpf+0xbb8/0x2588 [130.645175] [<90000000032b8388>] sys_bpf+0x20/0x2c [130.645259] [<9000000003f6ab38>] do_syscall+0x7c/0x94 [130.645369] [<9000000003121c5c>] handle_syscall+0xbc/0x158 [130.645507] [130.645539] Code: 380839f6 380831f9 28412bae <24000ca6> 004081ad 0014cb50 004083e8 02bff34c 58008e91 [130.645729] [130.646418] ---[end trace 0000000000000000]--- On my machine, which has CONFIG_PAGE_SIZE_16KB=y, the test failed at loading a BPF prog with 2039 instructions: prog = (struct bpf_prog *)ffff80001b894000 insn = (struct bpf_insn *)(prog->insnsi)fff ---truncated---	7.8	Mc De
CVE-2023-52452	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix accesses to uninit stack slots Privileged programs are supposed to be able to read uninitialized stack memory (ever since 6715df8d5) but, before this patch, these accesses were permitted inconsistently. In particular, accesses were permitted above state->allocated_stack, but not below it. In other words, if the stack was already "large enough", the access was permitted, but otherwise the access was rejected instead of being allowed to "grow the stack". This undesired rejection was happening in two places: - in check_stack_slot_within_bounds() - in check_stack_range_initialized() This patch arranges for these accesses to be permitted. A bunch of tests that were relying on the old rejection had to change; all of them were changed to add also run unprivileged, in which case the old behavior persists. One tests couldn't be updated - global_func16 - because it can't run unprivileged for other reasons. This patch also fixes the tracking of the stack size for variable-offset reads. This second fix is bundled in the same commit as the first one because they're inter-related. Before this patch, writes to the stack using registers containing a variable offset (as opposed to registers with fixed, known values) were not properly contributing to the function's needed stack size. As a result, it was possible for a program to verify, but then to attempt to read out-of-bounds data at runtime because a too small stack had been allocated for it. Each function tracks the size of the stack it needs in bpf_subprog_info.stack_depth, which is maintained by update_stack_depth(). For regular memory accesses, check_mem_access() was calling update_state_depth() but it was passing in only the fixed part of the offset register, ignoring the variable offset. This was incorrect; the minimum possible value of that register should be used instead. This tracking is now fixed by centralizing the tracking of stack size in grow_stack_state(), and by lifting the calls to grow_stack_state() to check_stack_access_within_bounds() as suggested by Andrii. The code is now simpler and more convincingly tracks the correct maximum stack size. check_stack_range_initialized() can now rely on enough stack having been allocated for the access; this helps with the fix for the first issue. A few tests were changed to also check the stack depth computation. The one that fails without this patch is verifier_var_off:stack_write_priv_vs_unpriv.	7.8	Mc De
CVE-2024-0197	A flaw in the installer for Thales SafeNet Sentinel HASP LDK prior to 9.16 on Windows allows an attacker to escalate their privilege level via local access.	7.8	Mc De

CVE Number	Description	Base Score	Re
CVE-2023-52451	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/memhp: Fix access beyond end of drmem array dlpar_memory_remove_by_index() may access beyond the bounds of the drmem lmb array when the LMB lookup fails to match an entry with the given DRC index. When the search fails, the cursor is left pointing to &drmem_info->lmbs[drmem_info->n_lmbs], which is one element past the last valid entry in the array. The debug message at the end of the function then dereferences this pointer: pr_debug("Failed to hot-remove memory at %llx\n", lmb->base_addr); This was found by inspection and confirmed with KASAN: pseries-hotplug-mem: Attempting to hot-remove LMB, drc index 1234 == BUG: KASAN: slab-out-of-bounds in dlpar_memory+0x298/0x1658 Read of size 8 at addr c000000364e97fd0 by task bash/949 dump_stack_lvl+0xa4/0xfc (unreliable) print_report+0x214/0x63c kasan_report+0x140/0x2e0 __asan_load8+0xa8/0xe0 dlpar_memory+0x298/0x1658 handle_dlpar_errorlog+0x130/0x1d0 dlpar_store+0x18c/0x3e0 kobj_attr_store+0x68/0xa0 sysfs_kf_write+0xc4/0x110 kernfs_fop_write_iter+0x26c/0x390 vfs_write+0x2d4/0x4e0 ksys_write+0xac/0x1a0 system_call_exception+0x268/0x530 system_call_vectored_common+0x15c/0x2ec Allocated by task 1: kasan_save_stack+0x48/0x80 kasan_set_track+0x34/0x50 kasan_save_alloc_info+0x34/0x50 __kasan_kmalloc+0xd0/0x120 __kmalloc+0x8c/0x320 kmalloc_array.constprop.0+0x48/0x5c drmem_init+0x2a0/0x41c do_one_initcall+0xe0/0x5c0 kernel_init_freeable+0x4ec/0x5a0 kernel_init+0x30/0x1e0 ret_from_kernel_user_thread+0x14/0x1c The buggy address belongs to the object at c000000364e80000 which belongs to the cache kmalloc-128k of size 131072 The buggy address is located 0 bytes to the right of allocated 98256-byte region [c000000364e80000, c000000364e97fd0) == pseries-hotplug-mem: Failed to hot-remove memory at 0 Log failed lookups with a separate message and dereference the cursor only when it points to a valid entry.	7.8	Mo De
CVE-2023-52446	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a race condition between btf_put() and map_free() When running `./test_progs -j` in my local vm with latest kernel, I once hit a kasan error like below: [1887.184724] BUG: KASAN: slab-use-after-free in bpf_rb_root_free+0x1f8/0x2b0 [1887.185599] Read of size 4 at addr ffff888106806910 by task kworker/u12:2/2830 [1887.186498] [1887.186712] CPU: 3 PID: 2830 Comm: kworker/u12:2 Tainted: G OEL 6.7.0-rc3-00699-g90679706d486-dirty #494 [1887.188034] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 [1887.189618] Workqueue: events_unbound bpf_map_free_deferred [1887.190341] Call Trace: [1887.190666] <TASK> [1887.190949] dump_stack_lvl+0xac/0xe0 [1887.191423] ? nf_tcp_handle_invalid+0x1b0/0x1b0 [1887.192019] ? panic+0x3c0/0x3c0 [1887.192449] print_report+0x14f/0x720 [1887.192930] ? preempt_count_sub+0x1c/0xd0 [1887.193459] ? __virt_addr_valid+0xac/0x120 [1887.194004] ? bpf_rb_root_free+0x1f8/0x2b0 [1887.194572] kasan_report+0xc3/0x100 [1887.195085] ? bpf_rb_root_free+0x1f8/0x2b0 [1887.195668] bpf_rb_root_free+0x1f8/0x2b0 [1887.196183] ? __bpf_obj_drop_impl+0xb0/0xb0 [1887.196736] ? preempt_count_sub+0x1c/0xd0 [1887.197270] ? preempt_count_sub+0x1c/0xd0 [1887.197802] ? _raw_spin_unlock+0x1f/0x40 [1887.198319] bpf_obj_free_fields+0x1d4/0x260 [1887.198883] array_map_free+0x1a3/0x260 [1887.199380] bpf_map_free_deferred+0x7b/0xe0 [1887.199943] process_scheduled_works+0x3a2/0x6c0 [1887.200549] worker_thread+0x633/0x890 [1887.201047] ? __kthread_parkme+0xd7/0xf0 [1887.201574] ? kthread+0x102/0x1d0 [1887.202020] kthread+0x1ab/0x1d0 [1887.202447] ? pr_cont_work+0x270/0x270 [1887.202954] ? kthread_blkcg+0x50/0x50 [1887.203444] ret_from_fork+0x34/0x50 [1887.203914] ? kthread_blkcg+0x50/0x50 [1887.204397] ret_from_fork_asm+0x11/0x20 [1887.204913] </TASK> [1887.204913] </TASK> [1887.205209] [1887.205416] Allocated by task 2197: [1887.205881] kasan_set_track+0x3f/0x60 [1887.206366] __kasan_kmalloc+0x6e/0x80 [1887.206856] __kmalloc+0xac/0x1a0 [1887.207293] btf_parse_fields+0xa15/0x1480 [1887.207836] btf_parse_struct_metas+0x566/0x670 [1887.208387] btf_new_fd+0x294/0x4d0 [1887.208851] __sys_bpf+0x4ba/0x600 [1887.209292] __x64_sys_bpf+0x41/0x50 [1887.209762] do_syscall_64+0x4c/0xf0 [1887.210222] entry_SYSCALL_64_after_hwframe+0x63/0x6b [1887.210868] [1887.211074] Freed by task 36: [1887.211460] kasan_set_track+0x3f/0x60 [1887.211951] kasan_save_free_info+0x28/0x40 [1887.212485] ____kasan_slab_free+0x101/0x180 [1887.213027] __kmem_cache_free+0xe4/0x210 [1887.213514] btf_free+0x5b/0x130 [1887.213918] rcu_core+0x638/0xcc0 [1887.214347] __do_softirq+0x114/0x37e The error happens at bpf_rb_root_free+0x1f8/0x2b0: 00000000000034c0 <bpf_rb_root_free>: ; { 34c0: f3 0f 1e fa endbr64 34c4: e8 00 00 00 00 callq 0x34c9 <bpf_rb_root_free+0x9> 34c9: 55 pushq %rbp 34ca: 48 89 e5 movq %rsp, %rbp ... ; if (rec && rec->refcount_off >= 0 && 36aa: 4d 85 ed testq %r13, %r13 36ad: 74 a9 je 0x3658 <bpf_rb_root_free+0x198> 36af: 49 8d 7d 10 leaq 0x10(%r13), %rdi 36b3: e8 00 00 00 00 callq 0x36b8 <bpf_rb_root_free+0x1f8> <==== kasan function 36b8: 45 8b 7d 10 movl 0x10(%r13), %r15d <==== use-after-free load 36bc: 45 85 ff testl %r15d, %r15d 36bf: 78 8c js 0x364d <bpf_rb_root_free+0x18d> So the problem ---truncated---	7.8	Mo De
CVE-2023-52445	In the Linux kernel, the following vulnerability has been resolved: media: pvrusb2: fix use after free on context disconnection Upon module load, a kthread is created targeting the pvr2_context_thread_func function, which may call pvr2_context_destroy and thus call kfree() on the context object. However, that might happen before the usb hub_event handler is able to notify the driver. This patch adds a sanity check before the invalid read reported by syzbot, within the context disconnection call stack.	7.8	Mo De
CVE-2021-46950	In the Linux kernel, the following vulnerability has been resolved: md/raid1: properly indicate failure when ending a failed write request This patch addresses a data corruption bug in raid1 arrays using bitmaps. Without this fix, the bitmap bits for the failed I/O end up being cleared. Since we are in the failure leg of raid1_end_write_request, the request either needs to be retried (R1BIO_WriteError) or failed (R1BIO_Degraded).	7.8	Mo De
CVE-2023-52444	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid dirent corruption As AI reported in link[1]: f2fs_rename() ... if (old_dir != new_dir && !whiteout) f2fs_set_link(old_inode, old_dir_entry, old_dir_page, new_dir); else f2fs_put_page(old_dir_page, 0); You want correct inumber in the ".." link. And cross-directory rename does move the source to new parent, even if you'd been asked to leave a whiteout in the old place. [1] https://lore.kernel.org/all/20231017055040.GN800259@ZenIV/ With below testcase, it may cause dirent corruption, due to it missed to call f2fs_set_link() to update ".." link to new directory. - mkdir -p dir/foo - renameat2 -w dir/foo bar [ASSERT] (__chk_dots_dentries:1421) --> Bad inode number[0x4] for '..', parent parent ino is [0x3] [FSCK] other corrupted bugs [Fail]	7.8	Mo De
CVE-2024-24096	Code-projects Computer Book Store 1.0 is vulnerable to SQL Injection via BookSBIN.	7.8	Mo De
CVE-2024-26283	An attacker could have executed unauthorized scripts on top origin sites using a JavaScript URI when opening an external URL with a custom Firefox scheme. This vulnerability affects Firefox for iOS < 123.	7.8	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46936	In the Linux kernel, the following vulnerability has been resolved: net: fix use-after-free in tw_timer_handler A real world panic issue was found as follow in Linux 5.4. BUG: unable to handle page fault for address: ffffde49a863de28 PGD 7e6fe62067 P4D 7e6fe62067 PUD 7e6fe63067 PMD f51e064067 PTE 0 RIP: 0010:tw_timer_handler+0x20/0x40 Call Trace: <IRQ> call_timer_fn+0x2b/0x120 run_timer_softirq+0x1ef/0x450 __do_softirq+0x10d/0x2b8 irq_exit+0xc7/0xd0 smp_apic_timer_interrupt+0x68/0x120 apic_timer_interrupt+0xf/0x20 This issue was also reported since 2017 in the thread [1], unfortunately, the issue was still can be reproduced after fixing DCCP. The ipv4_mib_exit_net is called before tcp_sk_exit_batch when a net namespace is destroyed since tcp_sk_ops is registered befrore ipv4_mib_ops, which means tcp_sk_ops is in the front of ipv4_mib_ops in the list of pernet_list. There will be a use-after-free on net->mib.net_statistics in tw_timer_handler after ipv4_mib_exit_net if there are some inflight time-wait timers. This bug is not introduced by commit f2bf415cfed7 ("mib: add net to NET_ADD_STATS_BH") since the net_statistics is a global variable instead of dynamic allocation and freeing. Actually, commit 61a7e26028b9 ("mib: put net statistics on struct net") introduces the bug since it put net statistics on struct net and free it when net namespace is destroyed. Moving init_ipv4_mibs() to the front of tcp_init() to fix this bug and replace pr_crit() with panic() since continuing is meaningless when init_ipv4_mibs() fails. [1] https://groups.google.com/g/syzkaller/c/p1tn-_Kc6l4/m/smuL_FMAAgAJ?pli=1	7.8	Mo De
CVE-2023-7016	A flaw in Thales SafeNet Authentication Client prior to 10.8 R10 on Windows allows an attacker to execute code at a SYSTEM level via local access.	7.8	Mo De
CVE-2023-5993	A flaw in the Windows Installer in Thales SafeNet Authentication Client prior to 10.8 R10 on Windows allows an attacker to escalate their privilege level via local access.	7.8	Mo De
CVE-2023-52468	In the Linux kernel, the following vulnerability has been resolved: class: fix use-after-free in class_register() The lock_class_key is still registered and can be found in lock_keys_hash hlist after subsys_private is freed in error handler path.A task who iterate over the lock_keys_hash later may cause use-after-free.So fix that up and unregister the lock_class_key before kfree(cp). On our platform, a driver fails to kset_register because of creating duplicate filename '/class/xxx'.With Kasan enabled, it prints a invalid-access bug report. KASAN bug report: BUG: KASAN: invalid-access in lockdep_register_key+0x19c/0x1bc Write of size 8 at addr 15ffff808b8c0368 by task modprobe/252 Pointer tag: [15], memory tag: [fe] CPU: 7 PID: 252 Comm: modprobe Tainted: G W 6.6.0-mainline-maybe-dirty #1 Call trace: dump_backtrace+0x1b0/0x1e4 show_stack+0x2c/0x40 dump_stack_lvl+0xac/0xe0 print_report+0x18c/0x4d8 kasan_report+0xe8/0x148 __hwasan_store8_noabort+0x88/0x98 lockdep_register_key+0x19c/0x1bc class_register+0x94/0x1ec init_module+0xbc/0xf48 [rfkill] do_one_initcall+0x17c/0x72c do_init_module+0x19c/0x3f8 ... Memory state around the buggy address: ffffff808b8c0100: 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a 8a ffffff808b8c0200: 8a 8a 8a 8a 8a 8a 8a fe fe fe fe fe fe fe fe >ffffff808b8c0300: fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe ^ ffffff808b8c0400: 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 As CONFIG_KASAN_GENERIC is not set, Kasan reports invalid-access not use-after-free here.In this case, modprobe is manipulating the corrupted lock_keys_hash hlish where lock_class_key is already freed before. It's worth noting that this only can happen if lockdep is enabled, which is not true for normal system.	7.8	Mo De
CVE-2019-25162	In the Linux kernel, the following vulnerability has been resolved: i2c: Fix a potential use after free Free the adap structure only after we are done using it. This patch just moves the put_device() down a bit to avoid the use after free. [wsa: added comment to the code, added Fixes tag]	7.8	Mo De
CVE-2023-52457	In the Linux kernel, the following vulnerability has been resolved: serial: 8250: omap: Don't skip resource freeing if pm_runtime_resume_and_get() failed Returning an error code from .remove() makes the driver core emit the little helpful error message: remove callback returned a non-zero value. This will be ignored. and then remove the device anyhow. So all resources that were not freed are leaked in this case. Skipping serial8250_unregister_port() has the potential to keep enough of the UART around to trigger a use-after-free. So replace the error return (and with it the little helpful error message) by a more useful error message and continue to cleanup.	7.8	Mo De
CVE-2023-52464	In the Linux kernel, the following vulnerability has been resolved: EDAC/thunderx: Fix possible out-of-bounds string access Enabling -Wstringop-overflow globally exposes a warning for a common bug in the usage of strncat(): drivers/edac/thunderx_edac.c: In function 'thunderx_ocx_com_threaded_isr': drivers/edac/thunderx_edac.c:1136:17: error: 'strncat' specified bound 1024 equals destination size [-Werror=stringop-overflow=] 1136 | strncat(msg, other, OCX_MESSAGE_SIZE); | ^~~~~~~ ... 1145 | strncat(msg, other, OCX_MESSAGE_SIZE); ... 1150 | strncat(msg, other, OCX_MESSAGE_SIZE); ... Apparently the author of this driver expected strncat() to behave the way that strlcat() does, which uses the size of the destination buffer as its third argument rather than the length of the source buffer. The result is that there is no check on the size of the allocated buffer. Change it to strlcat(). [bp: Trim compiler output, fixup commit message.]	7.8	Mo De
CVE-2024-26599	In the Linux kernel, the following vulnerability has been resolved: pwm: Fix out-of-bounds access in of_pwm_single_xlate() With args->args_count == 2 args->args[2] is not defined. Actually the flags are contained in args->args[1].	7.8	Mo De
CVE-2023-52455	In the Linux kernel, the following vulnerability has been resolved: iommu: Don't reserve 0-length IOVA region When the bootloader/firmware doesn't setup the framebuffers, their address and size are 0 in "iommu-addresses" property. If IOVA region is reserved with 0 length, then it ends up corrupting the IOVA rbtree with an entry which has pfn_hi < pfn_lo. If we intend to use display driver in kernel without framebuffer then it's causing the display IOMMU mappings to fail as entire valid IOVA space is reserved when address and length are passed as 0. An ideal solution would be firmware removing the "iommu-addresses" property and corresponding "memory-region" if display is not present. But the kernel should be able to handle this by checking for size of IOVA region and skipping the IOVA reservation if size is 0. Also, add a warning if firmware is requesting 0-length IOVA region reservation.	7.8	Mo De
CVE-2021-46966	In the Linux kernel, the following vulnerability has been resolved: ACPI: custom_method: fix potential use-after-free issue In cm_write(), buf is always freed when reaching the end of the function. If the requested count is less than table.length, the allocated buffer will be freed but subsequent calls to cm_write() will still try to access it. Remove the unconditional kfree(buf) at the end of the function and set the buf to NULL in the -EINVAL error path to match the rest of function.	7.8	Mo De
CVE-2024-26598	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic-its: Avoid potential UAF in LPI translation cache There is a potential UAF scenario in the case of an LPI translation cache hit racing with an operation that invalidates the cache, such as a DISCARD ITS command. The root of the problem is that vgic_its_check_cache() does not elevate the refcount on the vgic_irq before dropping the lock that serializes refcount changes. Have vgic_its_check_cache() raise the refcount on the returned vgic_irq and add the corresponding decrement after queueing the interrupt.	7.8	Mo De
CVE-2022-48626	In the Linux kernel, the following vulnerability has been resolved: moxart: fix potential use-after-free on remove path It was reported that the mmc host structure could be accessed after it was freed in moxart_remove(), so fix this by saving the base register of the device and using it instead of the pointer dereference.	7.8	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26582	In the Linux kernel, the following vulnerability has been resolved: net: tls: fix use-after-free with partial reads and async decrypt tls_decrypt_sg doesn't take a reference on the pages from clear_skb, so the put_page() in tls_decrypt_done releases them, and we trigger a use-after-free in process_rx_list when we try to read from the partially-read skb.	7.8	Mo De
CVE-2024-0410	An authorization bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.7.6, 16.8 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict.	7.7	Mo De
CVE-2024-25840	In the module "Account Manager l Sales Representative & Dealers l CRM" (prestasalesmanager) up to 9.0 from Presta World for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack.	7.5	Mo De
CVE-2024-23131	A maliciously crafted STP file, when parsed in ASMIMPORT229A.dll, ASMKERN228A.dll, ASMkern229A.dll or ASMDATAX228A.dll through Autodesk applications, can lead to a memory corruption vulnerability by write access violation. This vulnerability, in conjunction with other vulnerabilities, can lead to code execution in the context of the current process.	7.5	Mo De
CVE-2024-23130	A maliciously crafted SLDASM or SLDPRT file, when parsed in ODXSW_DLL.dll through Autodesk applications, can lead to a memory corruption vulnerability by write access violation. This vulnerability, in conjunction with other vulnerabilities, can lead to code execution in the context of the current process.	7.5	Mo De
CVE-2024-23129	A maliciously crafted MODEL 3DM, STP, or SLDASM file, when in opennurbs.dll parsed through Autodesk applications, can lead to a memory corruption vulnerability by write access violation. This vulnerability, in conjunction with other vulnerabilities, can lead to code execution in the context of the current process.	7.5	Mo De
CVE-2024-23128	A maliciously crafted MODEL file, when parsed in libodxdll.dll and ASMDATAX229A.dll through Autodesk applications, can lead to a memory corruption vulnerability by write access violation. This vulnerability, in conjunction with other vulnerabilities, can lead to code execution in the context of the current process.	7.5	Mo De
CVE-2024-23127	A maliciously crafted MODEL, SLDPRT, or SLDASM file, when parsed in ODXSW_DLL.dll and libodxdll.dll through Autodesk applications, can be used to cause a Heap-based Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-23124	A maliciously crafted STP file in ASMIMPORT228A.dll when parsed through Autodesk AutoCAD can force an Out-of-Bound Write. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-23126	A maliciously crafted CATPART file in CC5Dll.dll when parsed through Autodesk AutoCAD can be used to cause a Stack-based Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-23125	A maliciously crafted SLDPRT file when parsed ODXSW_DLL.dll through Autodesk AutoCAD can be used to cause a Stack-based Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-23123	A maliciously crafted CATPART file, when parsed in CC5Dll.dll and ASMBASE228A.dll through Autodesk applications, can force an Out-of-Bound Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-23122	A maliciously crafted 3DM file, when parsed in opennurbs.dll through Autodesk applications, can force an Out-of-Bound Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-23121	A maliciously crafted MODEL file when parsed in libodxdll.dll through Autodesk applications can force an Out-of-Bound Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-25469	SQL Injection vulnerability in CRMEB crmeb_java v.1.3.4 and before allows a remote attacker to obtain sensitive information via the latitude and longitude parameters in the api/front/store/list component.	7.5	Mo De
CVE-2024-23132	A maliciously crafted STP file in atf_dwg_consumer.dll when parsed through Autodesk AutoCAD could lead to a memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.5	Mo De
CVE-2024-23134	A maliciously crafted IGS file in tbb.dll when parsed through Autodesk AutoCAD can be used in user-after-free vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	7.5	Mo De
CVE-2024-23133	A maliciously crafted STP file in ASMDATAX228A.dll when parsed through Autodesk AutoCAD could lead to a memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.5	Mo De
CVE-2023-42835	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1. An attacker may be able to access user data.	7.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-24309	In the module "Survey TMA" (ecomiz_survey_tma) up to version 2.0.0 from Ecomiz for PrestaShop, a guest can download personal information without restriction.	7.5	Mc De
CVE-2023-3966	A flaw was found in Open vSwitch where multiple versions are vulnerable to crafted Geneve packets, which may result in a denial of service and invalid memory accesses. Triggering this issue requires that hardware offloading via the netlink path is enabled.	7.5	Mc De
CVE-2024-1104	An unauthenticated remote attacker can bypass the brute force prevention mechanism and disturb the webservice for all users.	7.5	Mc De
CVE-2024-27356	An issue was discovered on certain GL-iNet devices. Attackers can download files such as logs via commands, potentially obtaining critical user information. This affects MT6000 4.5.5, XE3000 4.4.4, X3000 4.4.5, MT3000 4.5.0, MT2500 4.5.0, AXT1800 4.5.0, AX1800 4.5.0, A1300 4.5.0, S200 4.1.4-0300, X750 4.3.7, SFT1200 4.3.7, XE300 4.3.7, MT1300 4.3.10, AR750 4.3.10, AR750S 4.3.10, AR300M 4.3.10, AR300M16 4.3.10, B1300 4.3.10, MT300N-v2 4.3.10, X300B 3.217, S1300 3.216, SF1200 3.216, MV1000 3.216, N300 3.216, B2200 3.216, and X1200 3.203.	7.5	Mc De
CVE-2023-29180	A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.3, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to denial of service via specially crafted HTTP requests.	7.5	Mc De
CVE-2024-1622	Due to a mistake in error checking, Routinator will terminate when an incoming RTR connection is reset by the peer too quickly after opening.	7.5	Mc De
CVE-2023-52161	The Access Point functionality in eapol_auth_key_handle in eapol.c in iNet wireless daemon (IWD) before 2.14 allows attackers to gain unauthorized access to a protected Wi-Fi network. An attacker can complete the EAPOL handshake by skipping Msg2/4 and instead sending Msg4/4 with an all-zero key.	7.5	Mc De
CVE-2024-22778	HackMD CodiMD <2.5.2 is vulnerable to Denial of Service.	7.5	Mc De
CVE-2024-24478	An issue in Wireshark before 4.2.0 allows a remote attacker to cause a denial of service via the packet-bgp.c, dissect_bgp_open(tvbuff_t*tvb, proto_tree*tree, packet_info*pinfo), optlen components. NOTE: this is disputed by the vendor because neither release 4.2.0 nor any other release was affected.	7.5	Mc De
CVE-2024-26455	fluent-bit 2.2.2 contains a Use-After-Free vulnerability in /fluent-bit/plugins/custom_calyptia/calyptia.c.	7.5	Mc De
CVE-2024-27132	Insufficient sanitization in MLflow leads to XSS when running an untrusted recipe. This issue leads to a client-side RCE when running an untrusted recipe in Jupyter Notebook. The vulnerability stems from lack of sanitization over template variables.	7.5	Mc De
CVE-2024-27133	Insufficient sanitization in MLflow leads to XSS when running a recipe that uses an untrusted dataset. This issue leads to a client-side RCE when running the recipe in Jupyter Notebook. The vulnerability stems from lack of sanitization over dataset table fields.	7.5	Mc De
CVE-2024-25768	OpenDMARC 1.4.2 contains a null pointer dereference vulnerability in /OpenDMARC/libopendmarc/opendmarc_policy.c.	7.5	Mc De
CVE-2024-23137	A maliciously crafted STP or SLDPRT file, when parsed in ODXSW_DLL.dll through Autodesk applications, can be used to uninitialized variables. This vulnerability, along with other vulnerabilities, can lead to code execution in the current process.	7.5	Mc De
CVE-2024-23136	A maliciously crafted STP file in ASMKERN228A.dll when parsed through Autodesk AutoCAD can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	7.5	Mc De
CVE-2024-23135	A maliciously crafted SLDPRT file in ASMkern228A.dll when parsed through Autodesk AutoCAD can be used in user-after-free vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	7.5	Mc De
CVE-2024-23120	A maliciously crafted STP and STEP file when parsed in ASMIMPORT228A.dll and ASMIMPORT229A.dll and through Autodesk applications can force an Out-of-Bound Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mc De
CVE-2024-22201	Jetty is a Java based web server and servlet engine. An HTTP/2 SSL connection that is established and TCP congested will be leaked when it times out. An attacker can cause many connections to end up in this state, and the server may run out of file descriptors, eventually causing the server to stop accepting new connections from valid clients. The vulnerability is patched in 9.4.54, 10.0.20, 11.0.20, and 12.0.6.	7.5	Mc De
CVE-2022-45177	An issue was discovered in LIVEBOX Collaboration vDesk through v031. An Observable Response Discrepancy can occur under the /api/v1/vdeskintegration/user/isenableuser endpoint, the /api/v1/sharedsearch?search={NAME]+{SURNAME] endpoint, and the /login endpoint. The web application provides different responses to incoming requests in a way that reveals internal state information to an unauthorized actor outside of the intended control sphere.	7.5	Mc De

CVE Number	Description	Base Score	Re
CVE-2024-25461	Directory Traversal vulnerability in Terrasoft, Creatio Terrasoft CRM v.7.18.4.1532 allows a remote attacker to obtain sensitive information via a crafted request to the terrasoft.axd component.	7.5	Mc De
CVE-2023-49960	In Indo-Sol PROFINET-INspektor NT through 2.4.0, a path traversal vulnerability in the httpuploadd service of the firmware allows remote attackers to write to arbitrary files via a crafted filename parameter in requests to the /upload endpoint.	7.5	Mc De
CVE-2023-6585	The WP JobSearch WordPress plugin before 2.3.4 does not validate files to be uploaded, which could allow unauthenticated attackers to upload arbitrary files such as PHP on the server	7.5	Mc De
CVE-2024-26130	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Starting in version 38.0.0 and prior to version 42.0.4, if `pkcs12.serialize_key_and_certificates` is called with both a certificate whose public key did not match the provided private key and an `encryption_algorithm` with `hmac_hash` set (via `PrivateFormat.PKCS12.encryption_builder().hmac_hash(...)`, then a NULL pointer dereference would occur, crashing the Python process. This has been resolved in version 42.0.4, the first version in which a `ValueError` is properly raised.	7.5	Mc De
CVE-2024-23837	LibHTP is a security-aware parser for the HTTP protocol. Crafted traffic can cause excessive processing time of HTTP headers, leading to denial of service. This issue is addressed in 0.5.46.	7.5	Mc De
CVE-2024-27318	Versions of the package onnx before and including 1.15.0 are vulnerable to Directory Traversal as the external_data field of the tensor proto can have a path to the file which is outside the model current directory or user-provided directory. The vulnerability occurs as a bypass for the patch added for CVE-2022-25882.	7.5	Mc De
CVE-2024-23836	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Prior to versions 6.0.16 and 7.0.3, an attacker can craft traffic to cause Suricata to use far more CPU and memory for processing the traffic than needed, which can lead to extreme slow downs and denial of service. This vulnerability is patched in 6.0.16 or 7.0.3. Workarounds include disabling the affected protocol app-layer parser in the yaml and reducing the `stream.reassembly.depth` value helps reduce the severity of the issue.	7.5	Mc De
CVE-2024-25891	ChurchCRM 5.5.0 FRBidSheets.php is vulnerable to Blind SQL Injection (Time-based) via the CurrentFundraiser GET parameter.	7.5	Mc De
CVE-2024-1786	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DIR-600M C1 3.08. Affected by this issue is some unknown functionality of the component Telnet Service. The manipulation of the argument username leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254576. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	7.5	Mc De
CVE-2024-23835	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Prior to version 7.0.3, excessive memory use during pgsql parsing could lead to OOM-related crashes. This vulnerability is patched in 7.0.3. As workaround, users can disable the pgsql app layer parser.	7.5	Mc De
CVE-2024-27359	Certain WithSecure products allow a Denial of Service because the engine scanner can go into an infinite loop when processing an archive file. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, WithSecure Linux Security 64 12.0, WithSecure Linux Protection 12.0, and WithSecure Atlant 1.0.35-1.	7.5	Mc De
CVE-2024-24476	A buffer overflow in Wireshark before 4.2.0 allows a remote attacker to cause a denial of service via the pan/addr_resolv.c, and ws_manuf_lookup_str(), size components. NOTE: this is disputed by the vendor because neither release 4.2.0 nor any other release was affected.	7.5	Mc De
CVE-2024-24479	A Buffer Overflow in Wireshark before 4.2.0 allows a remote attacker to cause a denial of service via the wsutil/to_str.c, and format_fractional_part_nsecs components. NOTE: this is disputed by the vendor because neither release 4.2.0 nor any other release was affected.	7.5	Mc De
CVE-2023-7165	The JetBackup WordPress plugin before 2.0.9.9 doesn't use index files to prevent public directory listing of sensitive directories in certain configurations, which allows malicious actors to leak backup files.	7.5	Mc De
CVE-2024-27454	orjson.loads in orjson before 3.9.15 does not limit recursion for deeply nested JSON documents.	7.5	Mc De
CVE-2024-27507	libLAS 1.8.1 contains a memory leak vulnerability in /libLAS/apps/ts2las.cpp.	7.5	Mc De
CVE-2023-6584	The WP JobSearch WordPress plugin before 2.3.4 does not prevent attackers from logging-in as any users with the only knowledge of that user's email address.	7.5	Mc De
CVE-2024-27508	Atheme 7.2.12 contains a memory leak vulnerability in /atheme/src/crypto-benchmark/main.c.	7.5	Mc De

CVE Number	Description	Base Score	Re
CVE-2024-26142	Rails is a web-application framework. Starting in version 7.1.0, there is a possible ReDoS vulnerability in the Accept header parsing routines of Action Dispatch. This vulnerability is patched in 7.1.3.1. Ruby 3.2 has mitigations for this problem, so Rails applications using Ruby 3.2 or newer are unaffected.	7.5	Mo De
CVE-2024-0446	A maliciously crafted STP, CATPART or MODEL file when parsed in ASMKERN228A.dll and ASMdatax229A.dll through Autodesk applications can force an Out-of-Bound Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	Mo De
CVE-2024-25398	In Srelay (the SOCKS proxy and Relay) v.0.4.8p3, a specially crafted network payload can trigger a denial of service condition and disrupt the service.	7.5	Mo De
CVE-2024-21502	Versions of the package fastecdsa before 2.3.2 are vulnerable to Use of Uninitialized Variable on the stack, via the curvemath_mul function in src/curveMath.c, due to being used and interpreted as user-defined type. Depending on the variable's actual value it could be arbitrary free(), arbitrary realloc(), null pointer dereference and other. Since the stack can be controlled by the attacker, the vulnerability could be used to corrupt allocator structure, leading to possible heap exploitation. The attacker could cause denial of service by exploiting this vulnerability.	7.5	Mo De
CVE-2023-38844	SQL injection vulnerability in PMB v.7.4.7 and earlier allows a remote attacker to execute arbitrary code via the thesaurus parameter in export_skos.php.	7.5	Mo De
CVE-2022-25377	The ACME-challenge endpoint in Appwrite 0.5.0 through 0.12.x before 0.12.2 allows remote attackers to read arbitrary local files via ../ directory traversal. In order to be vulnerable, APP_STORAGE_CERTIFICATES/.well-known/acme-challenge must exist on disk. (This pathname is automatically created if the user chooses to install Let's Encrypt certificates via Appwrite.)	7.5	Mo De
CVE-2024-1474	In WS_FTP Server versions before 8.8.5, reflected cross-site scripting issues have been identified on various user supplied inputs on the WS_FTP Server administrative interface.	7.5	Mo De
CVE-2024-26147	Helm is a package manager for Charts for Kubernetes. Versions prior to 3.14.2 contain an uninitialized variable vulnerability when Helm parses index and plugin yaml files missing expected content. When either an `index.yaml` file or a plugins `plugin.yaml` file were missing all metadata a panic would occur in Helm. In the Helm SDK, this is found when using the `LoadIndexFile` or `DownloadIndexFile` functions in the `repo` package or the `LoadDir` function in the `plugin` package. For the Helm client this impacts functions around adding a repository and all Helm functions if a malicious plugin is added as Helm inspects all known plugins on each invocation. This issue has been resolved in Helm v3.14.2. If a malicious plugin has been added which is causing all Helm client commands to panic, the malicious plugin can be manually removed from the filesystem. If using Helm SDK versions prior to 3.14.2, calls to affected functions can use `recover` to catch the panic.	7.5	Mo De
CVE-2024-0819	Improper initialization of default settings in TeamViewer Remote Client prior version 15.51.5 for Windows, Linux and macOS, allow a low privileged user to elevate privileges by changing the personal password setting and establishing a remote connection to a logged-in admin account.	7.3	Mo De
CVE-2024-1820	A vulnerability was found in code-projects Crime Reporting System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file inchargelogin.php. The manipulation of the argument email/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254608.	7.3	Mo De
CVE-2024-1824	A vulnerability, which was classified as critical, has been found in CodeAstro House Rental Management System 1.0. Affected by this issue is some unknown functionality of the file signing.php. The manipulation of the argument uname/password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254612.	7.3	Mo De
CVE-2024-1876	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /psubmit.php. The manipulation of the argument pid with the input '+or+1%3d1%23 leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254724.	7.3	Mo De
CVE-2024-1833	A vulnerability was found in SourceCodester Employee Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /Account/login.php. The manipulation of the argument txtusername leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254624.	7.3	Mo De
CVE-2024-1826	A vulnerability has been found in code-projects Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file Source/librarian/user/student/login.php. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-254614 is the identifier assigned to this vulnerability.	7.3	Mo De
CVE-2024-1832	A vulnerability has been found in SourceCodester Complete File Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ of the component Admin Login Form. The manipulation of the argument username with the input torada%27+or+%271%27+%3D+%271%27+--+- leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254623.	7.3	Mo De
CVE-2024-1827	A vulnerability was found in code-projects Library System 1.0 and classified as critical. This issue affects some unknown processing of the file Source/librarian/user/teacher/login.php. The manipulation of the argument username/password leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254615.	7.3	Mo De
CVE-2024-1830	A vulnerability was found in code-projects Library System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file Source/librarian/user/student/lost-password.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254618 is the identifier assigned to this vulnerability.	7.3	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-1831	A vulnerability, which was classified as critical, was found in SourceCodester Complete File Management System 1.0. Affected is an unknown function of the file users/index.php of the component Login Form. The manipulation of the argument username with the input torada%27+or+%271%27+%3D+%271%27+--+- leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-254622 is the identifier assigned to this vulnerability.	7.3	Mo De
CVE-2024-1817	A vulnerability has been found in Demososo DM Enterprise Website Building System up to 2022.8 and classified as critical. Affected by this vulnerability is the function dmlogin of the file indexDM_load.php of the component Cookie Handler. The manipulation of the argument is_admin with the input y leads to improper authentication. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254605 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	Mo De
CVE-2024-1828	A vulnerability was found in code-projects Library System 1.0. It has been classified as critical. Affected is an unknown function of the file Source/librarian/user/teacher/registration.php. The manipulation of the argument email/idno/phone/username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254616.	7.3	Mo De
CVE-2024-1683	A DLL injection vulnerability exists where an authenticated, low-privileged local attacker could modify application files on the TIE Secure Relay host, which could allow for overriding of the configuration and running of new Secure Relay services.	7.3	Mo De
CVE-2024-1829	A vulnerability was found in code-projects Library System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file Source/librarian/user/student/registration.php. The manipulation of the argument email/regno/phone/username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254617 was assigned to this vulnerability.	7.3	Mo De
CVE-2021-33145	Uncaught exception in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	Mo De
CVE-2021-33161	Improper input validation in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	Mo De
CVE-2024-24323	SQL injection vulnerability in linlinjava litemall v.1.8.0 allows a remote attacker to obtain sensitive information via the nickname, consignee, orderSN, orderStatusArray parameters of the AdminOrdercontroller.java component.	7.2	Mo De
CVE-2024-1776	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to SQL Injection via the 'form-id' parameter in all versions up to, and including, 1.1.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	Mo De
CVE-2021-33158	Improper neutralization in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	Mo De
CVE-2023-52154	File Upload vulnerability in pmb/camera_upload.php in PMB 7.4.7 and earlier allows attackers to run arbitrary code via upload of crafted PHTML files.	7.2	Mo De
CVE-2024-26296	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	Mo De
CVE-2024-26295	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	Mo De
CVE-2024-26294	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	Mo De
CVE-2024-27283	A vulnerability was discovered in Veritas eDiscovery Platform before 10.2.5. The application administrator can upload potentially malicious files to arbitrary locations on the server on which the application is installed.	7.2	Mo De
CVE-2021-33157	Insufficient control flow management in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	Mo De
CVE-2024-27081	ESPHome is a system to control your ESP8266/ESP32. A security misconfiguration in the edit configuration file API in the dashboard component of ESPHome version 2023.12.9 (command line installation) allows authenticated remote attackers to read and write arbitrary files under the configuration directory rendering remote code execution possible. This vulnerability is patched in 2024.2.1.	7.2	Mo De
CVE-2024-24027	SQL Injection vulnerability in Likeshop before 2.5.7 allows attackers to run abitrary SQL commands via the function DistributionMemberLogic::getFansLists.	7.2	Mo De

CVE Number	Description	Base Score	Re
CVE-2023-52155	A SQL Injection vulnerability in /admin/sauvegarde/run.php in PMB 7.4.7 and earlier allows remote authenticated attackers to execute arbitrary SQL commands via the sauvegardes variable through the /admin/sauvegarde/run.php endpoint.	7.2	Mo De
CVE-2024-26297	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	Mo De
CVE-2024-26298	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	Mo De
CVE-2024-24714	Unrestricted Upload of File with Dangerous Type vulnerability in bPlugins LLC Icons Font Loader.This issue affects Icons Font Loader: from n/a through 1.1.4.	7.2	Mo De
CVE-2021-46954	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_frag: fix stack OOB read while fragmenting IPv4 packets when 'act_mirred' tries to fragment IPv4 packets that had been previously re-assembled using 'act_ct', splats like the following can be observed on kernels built with KASAN: BUG: KASAN: stack-out-of-bounds in ip_do_fragment+0x1b03/0x1f60 Read of size 1 at addr ffff888147009574 by task ping/947 CPU: 0 PID: 947 Comm: ping Not tainted 5.12.0-rc6+ #418 Hardware name: Red Hat KVM, BIOS 1.11.1-4.module+el8.1.0+4066+0f1aadab 04/01/2014 Call Trace: <IRQ> dump_stack+0x92/0xc1 print_address_description.constprop.7+0x1a/0x150 kasan_report.cold.13+0x7f/0x111 ip_do_fragment+0x1b03/0x1f60 sch_fragment+0x4bf/0xe40 tcf_mirred_act+0xc3d/0x11a0 [act_mirred] tcf_action_exec+0x104/0x3e0 fl_classify+0x49a/0x5e0 [cls_flower] tcf_classify_ingress+0x18a/0x820 __netif_receive_skb_core+0xae7/0x3340 __netif_receive_skb_one_core+0xb6/0x1b0 process_backlog+0x1ef/0x6c0 __napi_poll+0xaa/0x500 net_rx_action+0x702/0xac0 __do_softirq+0x1e4/0x97f do_softirq+0x71/0x90 </IRQ> __local_bh_enable_ip+0xdb/0xf0 ip_finish_output2+0x760/0x2120 ip_do_fragment+0x15a5/0x1f60 __ip_finish_output+0x4c2/0xea0 ip_output+0x1ca/0x4d0 ip_send_skb+0x37/0xa0 raw_sendmsg+0x1c4b/0x2d00 sock_sendmsg+0xdb/0x110 __sys_sendto+0x1d7/0x2b0 __x64_sys_sendto+0xdd/0x1b0 do_syscall_64+0x33/0x40 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f82e13853eb Code: 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 f3 0f 1e fa 48 8d 05 75 42 2c 00 41 89 ca 8b 00 85 c0 75 14 b8 2c 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 75 c3 0f 1f 40 00 41 57 4d 89 c7 41 56 41 89 RSP: 002b:00007ffe01fad888 EFLAGS: 00000246 ORIG_RAX: 000000000000002c RAX: ffffffffffffffda RBX: 00005571aac13700 RCX: 00007f82e13853eb RDX: 0000000000002330 RSI: 00005571aac13700 RDI: 0000000000000003 RBP: 0000000000002330 R08: 00005571aac10500 R09: 0000000000000010 R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffe01faefb0 R13: 00007ffe01fad890 R14: 00007ffe01fad980 R15: 00005571aac0f0a0 The buggy address belongs to the page: page:000000001dff2e03 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x147009 flags: 0x17ffffc0001000(reserved) raw: 0017ffffc0001000 ffffea00051c0248 ffffea00051c0248 0000000000000000 raw: 0000000000000000 0000000000000000 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff888147009400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff888147009480: f1 f1 f1 f1 04 f2 f2 f2 f2 f2 f2 f2 00 00 00 00 >ffff888147009500: 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 f2 f2 f2 ^ ffff888147009580: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff888147009600: 00 00 00 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 for IPv4 packets, sch_fragment() uses a temporary struct dst_entry. Then, in the following call graph: ip_do_fragment() ip_skb_dst_mtu() ip_dst_mtu_maybe_forward() ip_mtu_locked() the pointer to struct dst_entry is used as pointer to struct rtable: this turns the access to struct members like rt_mtu_locked into an OOB read in the stack. Fix this changing the temporary variable used for IPv4 packets in sch_fragment(), similarly to what is done for IPv6 few lines below.	7.1	Mo De
CVE-2024-23839	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Prior to 7.0.3, specially crafted traffic can cause a heap use after free if the ruleset uses the http.request_header or http.response_header keyword. The vulnerability has been patched in 7.0.3. To work around the vulnerability, avoid the http.request_header and http.response_header keywords.	7.1	Mo De
CVE-2021-46952	In the Linux kernel, the following vulnerability has been resolved: NFS: fs_context: validate UDP retrans to prevent shift out-of-bounds Fix shift out-of-bounds in xprt_calc_majortimeo(). This is caused by a garbage timeout (retrans) mount option being passed to nfs mount, in this case from syzkaller. If the protocol is XPRT_TRANSPORT_UDP, then 'retrans' is a shift value for a 64-bit long integer, so 'retrans' cannot be >= 64. If it is >= 64, fail the mount and return an error.	7.1	Mo De
CVE-2024-26482	An HTML injection vulnerability exists in the Edit Content Layout module of Kirby CMS v4.1.0. NOTE: the vendor disputes the significance of this report because some HTML formatting (such as with an H1 element) is allowed, but there is backend sanitization such that the reporter's mentioned "injecting malicious scripts" would not occur.	7.1	Mo De
CVE-2019-25160	In the Linux kernel, the following vulnerability has been resolved: netlabel: fix out-of-bounds memory accesses There are two array out-of-bounds memory accesses, one in cipso_v4_map_lvl_valid(), the other in netlbl_bitmap_walk(). Both errors are embarassingly simple, and the fixes are straightforward. As a FYI for anyone backporting this patch to kernels prior to v4.8, you'll want to apply the netlbl_bitmap_walk() patch to cipso_v4_bitmap_walk() as netlbl_bitmap_walk() doesn't exist before Linux v4.8.	7.1	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46955	In the Linux kernel, the following vulnerability has been resolved: openvswitch: fix stack OOB read while fragmenting IPv4 packets running openvswitch on kernels built with KASAN, it's possible to see the following splat while testing fragmentation of IPv4 packets: BUG: KASAN: stack-out-of-bounds in ip_do_fragment+0x1b03/0x1f60 Read of size 1 at addr ffff888112fc713c by task handler2/1367 CPU: 0 PID: 1367 Comm: handler2 Not tainted 5.12.0-rc6+ #418 Hardware name: Red Hat KVM, BIOS 1.11.1-4.module+el8.1.0+4066+0f1aadab 04/01/2014 Call Trace: dump_stack+0x92/0xc1 print_address_description.constprop.7+0x1a/0x150 kasan_report.cold.13+0x7f/0x111 ip_do_fragment+0x1b03/0x1f60 ovs_fragment+0x5bf/0x840 [openvswitch] do_execute_actions+0x1bd5/0x2400 [openvswitch] ovs_execute_actions+0xc8/0x3d0 [openvswitch] ovs_packet_cmd_execute+0xa39/0x1150 [openvswitch] genl_family_rcv_msg_doit.isra.15+0x227/0x2d0 genl_rcv_msg+0x287/0x490 netlink_rcv_skb+0x120/0x380 genl_rcv+0x24/0x40 netlink_unicast+0x439/0x630 netlink_sendmsg+0x719/0xbf0 sock_sendmsg+0xe2/0x110 ____sys_sendmsg+0x5ba/0x890 ___sys_sendmsg+0xe9/0x160 __sys_sendmsg+0xd3/0x170 do_syscall_64+0x33/0x40 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f957079db07 Code: c3 66 90 41 54 41 89 d4 55 48 89 f5 53 89 fb 48 83 ec 10 e8 eb ec ff ff 44 89 e2 48 89 ee 89 df 41 89 c0 b8 2e 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 35 44 89 c7 48 89 44 24 08 e8 24 ed ff ff 48 RSP: 002b:00007f956ce35a50 EFLAGS: 00000293 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 0000000000000019 RCX: 00007f957079db07 RDX: 0000000000000000 RSI: 00007f956ce35ae0 RDI: 0000000000000019 RBP: 00007f956ce35ae0 R08: 0000000000000000 R09: 00007f9558006730 R10: 0000000000000000 R11: 0000000000000293 R12: 0000000000000000 R13: 00007f956ce37308 R14: 00007f956ce35f80 R15: 00007f956ce35ae0 The buggy address belongs to the page: page:00000000af2a1d93 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x112fc7 flags: 0x17ffffc0000000() raw: 0017ffffc0000000 0000000000000000 dead000000000122 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected addr ffff888112fc713c is located in stack of task handler2/1367 at offset 180 in frame: ovs_fragment+0x0/0x840 [openvswitch] this frame has 2 objects: [32, 144) 'ovs_dst' [192, 424) 'ovs_rt' Memory state around the buggy address: ffff888112fc7000: f3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff888112fc7080: 00 f1 f1 f1 f1 00 00 00 00 00 00 00 00 00 00 00 >ffff888112fc7100: 00 00 00 f2 f2 f2 f2 f2 00 00 00 00 00 00 00 00 ^ ffff888112fc7180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff888112fc7200: 00 00 00 00 00 00 f2 f2 f2 00 00 00 00 00 00 00 for IPv4 packets, ovs_fragment() uses a temporary struct dst_entry. Then, in the following call graph: ip_do_fragment() ip_skb_dst_mtu() ip_dst_mtu_maybe_forward() ip_mtu_locked() the pointer to struct dst_entry is used as pointer to struct rtable: this turns the access to struct members like rt_mtu_locked into an OOB read in the stack. Fix this changing the temporary variable used for IPv4 packets in ovs_fragment(), similarly to what is done for IPv6 few lines below.	7.1	Mo De
CVE-2023-51747	Apache James prior to versions 3.8.1 and 3.7.5 is vulnerable to SMTP smuggling. A lenient behaviour in line delimiter handling might create a difference of interpretation between the sender and the receiver which can be exploited by an attacker to forge an SMTP envelop, allowing for instance to bypass SPF checks. The patch implies enforcement of CRLF as a line delimiter as part of the DATA transaction. We recommend James users to upgrade to non vulnerable versions.	7.1	Mo De
CVE-2024-24843	Cross-Site Request Forgery (CSRF) vulnerability in PowerPack Addons for Elementor PowerPack Pro for Elementor.This issue affects PowerPack Pro for Elementor: from n/a before 2.10.8.	7.1	Mo De
CVE-2024-26594	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate mech token in session setup If client send invalid mech token in session setup request, ksmbd validate and make the error if it is invalid.	7.1	Mo De
CVE-2024-25928	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sitepact.This issue affects Sitepact: from n/a through 1.0.5.	7.1	Mo De
CVE-2024-26597	In the Linux kernel, the following vulnerability has been resolved: net: qualcomm: rmnet: fix global oob in rmnet_policy The variable rmnet_link_ops assign a *bigger* maxtype which leads to a global out-of-bounds read when parsing the netlink attributes. See bug trace below: == BUG: KASAN: global-out-of-bounds in validate_nla lib/nlattr.c:386 [inline] BUG: KASAN: global-out-of-bounds in __nla_validate_parse+0x24af/0x2750 lib/nlattr.c:600 Read of size 1 at addr ffffffff92c438d0 by task syz-executor.6/84207 CPU: 0 PID: 84207 Comm: syz-executor.6 Tainted: G N 6.1.0 #3 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x8b/0xb3 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:284 [inline] print_report+0x172/0x475 mm/kasan/report.c:395 kasan_report+0xbb/0x1c0 mm/kasan/report.c:495 validate_nla lib/nlattr.c:386 [inline] __nla_validate_parse+0x24af/0x2750 lib/nlattr.c:600 __nla_parse+0x3e/0x50 lib/nlattr.c:697 nla_parse_nested_deprecated include/net/netlink.h:1248 [inline] __rtnl_newlink+0x50a/0x1880 net/core/rtnetlink.c:3485 rtnl_newlink+0x64/0xa0 net/core/rtnetlink.c:3594 rtnetlink_rcv_msg+0x43c/0xd70 net/core/rtnetlink.c:6091 netlink_rcv_skb+0x14f/0x410 net/netlink/af_netlink.c:2540 netlink_unicast_kernel net/netlink/af_netlink.c:1319 [inline] netlink_unicast+0x54e/0x800 net/netlink/af_netlink.c:1345 netlink_sendmsg+0x930/0xe50 net/netlink/af_netlink.c:1921 sock_sendmsg_nosec net/socket.c:714 [inline] sock_sendmsg+0x154/0x190 net/socket.c:734 ____sys_sendmsg+0x6df/0x840 net/socket.c:2482 ___sys_sendmsg+0x110/0x1b0 net/socket.c:2536 __sys_sendmsg+0xf3/0x1c0 net/socket.c:2565 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3b/0x90 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7fdcf2072359 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 f1 19 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fdcf13e3168 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007fdcf219ff80 RCX: 00007fdcf2072359 RDX: 0000000000000000 RSI: 0000000020000200 RDI: 0000000000000003 RBP: 00007fdcf20bd493 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fffbb8d7bdf R14: 00007fdcf13e3300 R15: 0000000000022000 </TASK> The buggy address belongs to the variable: rmnet_policy+0x30/0xe0 The buggy address belongs to the physical page: page:0000000065bdeb3c refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x155243 flags: 0x200000000001000(reservedlnode=0lzone=2) raw: 0200000000001000 ffffea00055490c8 ffffea00055490c8 0000000000000000 raw: 0000000000000000 0000000000000000 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffffffff92c43780: f9 f9 f9 f9 00 00 00 02 f9 f9 f9 f9 00 00 00 07 ffffffff92c43800: f9 f9 f9 f9 00 00 00 05 f9 f9 f9 f9 06 f9 f9 f9 >ffffffff92c43880: f9 f9 f9 f9 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9 ^ ffffffff92c43900: 00 00 00 00 00 00 00 07 f9 f9 f9 f9 f9 f9 f9 ffffffff92c43980: 00 00 00 07 f9 f9 f9 f9 00 00 00 05 f9 f9 f9 f9 According to the comment of `nla_parse_nested_deprecated`, the maxtype should be len(destination array) - 1. Hence use `IFLA_RMNET_MAX` here.	7.1	Mo De
CVE-2024-1714	An issue exists in all supported versions of IdentityIQ Lifecycle Manager that can result if an entitlement with a value containing leading or trailing whitespace is requested by an authenticated user in an access request.	7.1	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26282	Using an AMP url with a canonical element, an attacker could have executed JavaScript from an opened bookmarked page. This vulnerability affects Firefox for iOS < 123.	7.1	Mo De
CVE-2024-26593	In the Linux kernel, the following vulnerability has been resolved: i2c: i801: Fix block process call transactions According to the Intel datasheets, software must reset the block buffer index twice for block process call transactions: once before writing the outgoing data to the buffer, and once again before reading the incoming data from the buffer. The driver is currently missing the second reset, causing the wrong portion of the block buffer to be read.	7.1	Mo De
CVE-2024-25423	An issue in MAXON CINEMA 4D R2024.2.0 allows a local attacker to execute arbitrary code via a crafted c4d_base.xdl64 file.	7.0	Mo De
CVE-2024-22473	TRNG is used before initialization by ECDSA signing driver when exiting EM2/EM3 on Virtual Secure Vault (VSE) devices. This defect may allow Signature Spoofing by Key Recreation.This issue affects Gecko SDK through v4.4.0.	6.8	Mo De
CVE-2023-24416	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Arne Franken All In One Favicon.This issue affects All In One Favicon: from n/a through 4.7.	6.8	Mo De
CVE-2024-25117	php-svg-lib is a scalable vector graphics (SVG) file parsing/rendering library. Prior to version 0.5.2, php-svg-lib fails to validate that font-family doesn't contain a PHAR url, which might leads to RCE on PHP < 8.0, and doesn't validate if external references are allowed. This might leads to bypass of restrictions or RCE on projects that are using it, if they do not strictly revalidate the fontName that is passed by php-svg-lib. The `Style::fromAttributes(`), or the `Style::parseCssStyle()` should check the content of the `font-family` and prevents it to use a PHAR url, to avoid passing an invalid and dangerous `fontName` value to other libraries. The same check as done in the `Style::fromStyleSheets` might be reused. Libraries using this library as a dependency might be vulnerable to some bypass of restrictions, or even remote code execution, if they do not double check the value of the `fontName` that is passed by php-svg-lib. Version 0.5.2 contains a fix for this issue.	6.8	Mo De
CVE-2024-26586	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_acl_tcam: Fix stack corruption When tc filters are first added to a net device, the corresponding local port gets bound to an ACL group in the device. The group contains a list of ACLs. In turn, each ACL points to a different TCAM region where the filters are stored. During forwarding, the ACLs are sequentially evaluated until a match is found. One reason to place filters in different regions is when they are added with decreasing priorities and in an alternating order so that two consecutive filters can never fit in the same region because of their key usage. In Spectrum-2 and newer ASICs the firmware started to report that the maximum number of ACLs in a group is more than 16, but the layout of the register that configures ACL groups (PAGT) was not updated to account for that. It is therefore possible to hit stack corruption [1] in the rare case where more than 16 ACLs in a group are required. Fix by limiting the maximum ACL group size to the minimum between what the firmware reports and the maximum ACLs that fit in the PAGT register. Add a test case to make sure the machine does not crash when this condition is hit. [1] Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: mlxsw_sp_acl_tcam_group_update+0x116/0x120 [...] dump_stack_lvl+0x36/0x50 panic+0x305/0x330 __stack_chk_fail+0x15/0x20 mlxsw_sp_acl_tcam_group_update+0x116/0x120 mlxsw_sp_acl_tcam_group_region_attach+0x69/0x110 mlxsw_sp_acl_tcam_vchunk_get+0x492/0xa20 mlxsw_sp_acl_tcam_ventry_add+0x25/0xe0 mlxsw_sp_acl_rule_add+0x47/0x240 mlxsw_sp_flower_replace+0x1a9/0x1d0 tc_setup_cb_add+0xdc/0x1c0 fl_hw_replace_filter+0x146/0x1f0 fl_change+0xc17/0x1360 tc_new_tfilter+0x472/0xb90 rtnetlink_rcv_msg+0x313/0x3b0 netlink_rcv_skb+0x58/0x100 netlink_unicast+0x244/0x390 netlink_sendmsg+0x1e4/0x440 ____sys_sendmsg+0x164/0x260 ___sys_sendmsg+0x9a/0xe0 __sys_sendmsg+0x7a/0xc0 do_syscall_64+0x40/0xe0 entry_SYSCALL_64_after_hwframe+0x63/0x6b	6.7	Mo De
CVE-2024-22235	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with administrative access to the local system can escalate privileges to 'root'.	6.7	Mo De
CVE-2023-49114	A DLL hijacking vulnerability was identified in the Qognify VMS Client Viewer version 7.1 or higher, which allows local users to execute arbitrary code and obtain higher privileges via careful placement of a malicious DLL, if some specific pre-conditions are met.	6.7	Mo De
CVE-2023-6477	An issue has been discovered in GitLab EE affecting all versions starting from 16.5 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. When a user is assigned a custom role with admin_group_member permission, they may be able to make a group, other members or themselves Owners of that group, which may lead to privilege escalation.	6.7	Mo De
CVE-2023-52447	In the Linux kernel, the following vulnerability has been resolved: bpf: Defer the free of inner map when necessary When updating or deleting an inner map in map array or map htab, the map may still be accessed by non-sleepable program or sleepable program. However bpf_map_fd_put_ptr() decreases the ref-counter of the inner map directly through bpf_map_put(), if the ref-counter is the last one (which is true for most cases), the inner map will be freed by ops->map_free() in a kworker. But for now, most .map_free() callbacks don't use synchronize_rcu() or its variants to wait for the elapse of a RCU grace period, so after the invocation of ops->map_free completes, the bpf program which is accessing the inner map may incur use-after-free problem. Fix the free of inner map by invoking bpf_map_free_deferred() after both one RCU grace period and one tasks trace RCU grace period if the inner map has been removed from the outer map before. The deferment is accomplished by using call_rcu() or call_rcu_tasks_trace() when releasing the last ref-counter of bpf map. The newly-added rcu_head field in bpf_map shares the same storage space with work field to reduce the size of bpf_map.	6.7	Mo De
CVE-2021-46953	In the Linux kernel, the following vulnerability has been resolved: ACPI: GTDT: Don't corrupt interrupt mappings on watchdow probe failure When failing the driver probe because of invalid firmware properties, the GTDT driver unmaps the interrupt that it mapped earlier. However, it never checks whether the mapping of the interrupt actially succeeded. Even more, should the firmware report an illegal interrupt number that overlaps with the GIC SGI range, this can result in an IPI being unmapped, and subsequent fireworks (as reported by Dann Frazier). Rework the driver to have a slightly saner behaviour and actually check whether the interrupt has been mapped before unmapping things.	6.7	Mo De
CVE-2024-26300	A vulnerability in the guest interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	6.6	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26299	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	6.6	Mo De
CVE-2024-25082	Splinefont in FontForge through 20230101 allows command injection via crafted archives or compressed files.	6.5	Mo De
CVE-2023-6533	Malformed Device Reset Locally Command Class packets can be sent to the controller, causing the controller to assume the end device has left the network. After this, frames sent by the end device will not be acknowledged by the controller. This vulnerability exists in PC Controller v5.54.0, and earlier.	6.5	Mo De
CVE-2023-6640	Malformed S2 Nonce Get Command Class packets can be sent to crash PC Controller v5.54.0 and earlier.	6.5	Mo De
CVE-2024-26145	Discourse Calendar adds the ability to create a dynamic calendar in the first post of a topic on Discourse. Uninvited users are able to gain access to private events by crafting a request to update their attendance. This problem is resolved in commit dfc4fa15f340189f177a1d1ab2cc94ffed3c1190. As a workaround, one may use post visibility to limit access.	6.5	Mo De
CVE-2022-34357	IBM Cognos Analytics Mobile Server 11.1.7, 11.2.4, and 12.0.0 is vulnerable to Denial of Service due to due to weak or absence of rate limiting. By making unlimited http requests, it is possible for a single user to exhaust server resources over a period of time making service unavailable for other legitimate users. IBM X-Force ID: 230510.	6.5	Mo De
CVE-2024-25410	flusity-CMS 2.33 is vulnerable to Unrestricted Upload of File with Dangerous Type in update_setting.php.	6.5	Mo De
CVE-2023-29179	A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, Fortiproxy version 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 allows attacker to denial of service via specially crafted HTTP requests.	6.5	Mo De
CVE-2024-26301	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager.	6.5	Mo De
CVE-2024-1108	The Plugin Groups plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the admin_init() function in all versions up to, and including, 2.0.6. This makes it possible for unauthenticated attackers to change the settings of the plugin, which can also cause a denial of service due to a misconfiguration.	6.5	Mo De
CVE-2024-24721	An issue was discovered on Innovaphone PBX before 14r1 devices. The password form, used to authenticate, allows a Brute Force Attack through which an attacker may be able to access the administration panel	6.5	Mo De
CVE-2024-0387	The EDS-4000/G4000 Series prior to version 3.2 includes IP forwarding capabilities that users cannot deactivate. An attacker may be able to send requests to the product and have it forwarded to the target. An attacker can bypass access controls or hide the source of malicious requests.	6.5	Mo De
CVE-2024-25767	nanomq 0.21.2 contains a Use-After-Free vulnerability in /nanomq/nng/src/core/socket.c.	6.5	Mo De
CVE-2024-1671	Inappropriate implementation in Site Isolation in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	Mo De
CVE-2023-52160	The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP-TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks.	6.5	Mo De
CVE-2024-0407	Certain HP Enterprise LaserJet, and HP LaserJet Managed Printers are potentially vulnerable to information disclosure, when connections made by the device back to services enabled by some solutions may have been trusted without the appropriate CA certificate in the device's certificate store.	6.5	Mo De
CVE-2024-1890	Vulnerability whereby an attacker could send a malicious link to an authenticated operator, which could allow remote attackers to perform a clickjacking attack on Sunny WebBox firmware version 1.6.1 and earlier.	6.4	Mo De
CVE-2024-1323	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Post Type Grid Widget Title in all versions up to, and including, 2.10.30 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	Mo De
CVE-2024-1081	The 3D FlipBook – PDF Flipbook WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bookmark feature in all versions up to, and including, 1.15.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-1924	A vulnerability was found in CodeAstro Membership Management System 1.0. It has been classified as critical. This affects an unknown part of the file /get_membership_amount.php. The manipulation of the argument membershipTypeId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254859.	6.3	Mo De
CVE-2024-1878	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /myprofile.php. The manipulation of the argument id with the input 1%20or%201=1 leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254726 is the identifier assigned to this vulnerability.	6.3	Mo De
CVE-2024-1923	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0 and classified as critical. Affected by this issue is the function delete_class/delete_student of the file /ajax-api.php of the component List of Classes Page. The manipulation of the argument id with the input 1337'+or+1=1;--+ leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254858 is the identifier assigned to this vulnerability.	6.3	Mo De
CVE-2024-1781	A vulnerability was found in Totolink X6000R AX3000 9.4.0cu.852_20230719. It has been rated as critical. This issue affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component shttpd. The manipulation leads to command injection. The exploit has been disclosed to the public and may be used. The identifier VDB-254573 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	Mo De
CVE-2024-1877	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /cancel.php. The manipulation of the argument id with the input 1%20or%201=1 leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254725 was assigned to this vulnerability.	6.3	Mo De
CVE-2024-1926	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /app/ajax/search_sales_report.php. The manipulation of the argument customer leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254861 was assigned to this vulnerability.	6.3	Mo De
CVE-2024-22220	An issue was discovered in Terminalfour 7.4 through 7.4.0004 QP3 and 8 through 8.3.19, and Formbank through 2.1.10-FINAL. Unauthenticated Stored Cross-Site Scripting can occur, with resultant Admin Session Hijacking. The attack vectors are Form Builder and Form Preview.	6.3	Mo De
CVE-2024-1702	A vulnerability was found in keerti1924 PHP-MYSQL-User-Login-System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /edit.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254390 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	Mo De
CVE-2024-1875	A vulnerability was found in SourceCodester Complaint Management System 1.0 and classified as critical. This issue affects some unknown processing of the file users/register-complaint.php of the component Lodge Complaint Section. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254723.	6.3	Mo De
CVE-2024-1885	This vulnerability allows remote attackers to execute arbitrary code on the affected webOS of LG Signage.	6.3	Mo De
CVE-2024-22395	Improper access control vulnerability has been identified in the SMA100 SSL-VPN virtual office portal, which in specific conditions could potentially enable a remote authenticated attacker to associate another user's MFA mobile application.	6.3	Mo De
CVE-2023-51392	Ember ZNet between v7.2.0 and v7.4.0 used software AES-CCM instead of integrated hardware cryptographic accelerators, potentially increasing risk of electromagnetic and differential power analysis sidechannel attacks.	6.2	Mo De
CVE-2024-25385	An issue in flvmeta v.1.2.2 allows a local attacker to cause a denial of service via the flvmeta/src/flv.c:375:21 function in flv_close.	6.2	Mo De
CVE-2024-22543	An issue was discovered in Linksys Router E1700 1.0.04 (build 3), allows authenticated attackers to escalate privileges via a crafted GET request to the /goform/* URI or via the ExportSettings function.	6.1	Mo De
CVE-2024-1106	The Shariff Wrapper WordPress plugin before 4.6.10 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	6.1	Mo De
CVE-2024-26143	Rails is a web-application framework. There is a possible XSS vulnerability when using the translation helpers in Action Controller. Applications using translation methods like translate, or t on a controller, with a key ending in "_html", a :default key which contains untrusted user input, and the resulting string is used in a view, may be susceptible to an XSS vulnerability. The vulnerability is fixed in 7.1.3.1 and 7.0.8.1.	6.1	Mo De
CVE-2024-26468	A DOM based cross-site scripting (XSS) vulnerability in the component index.html of jstrieb/urlpages before commit 035b647 allows attackers to execute arbitrary Javascript via sending a crafted URL.	6.1	Mo De
CVE-2024-25166	Cross Site Scripting vulnerability in 71CMS v.1.0.0 allows a remote attacker to execute arbitrary code via the uploadfile action parameter in the controller.php file.	6.1	Mo De
CVE-2024-26542	Cross Site Scripting vulnerability in Bonitasoft, S.A v.7.14. and fixed in v.9.0.2, 8.0.3, 7.15.7, 7.14.8 allows attackers to execute arbitrary code via a crafted payload to the Groups Display name field.	6.1	Mo De

CVE Number	Description	Base Score	Re
CVE-2023-7202	The Fatal Error Notify WordPress plugin before 1.5.3 does not have authorisation and CSRF checks in its test_error AJAX action, allowing any authenticated users, such as subscriber to call it and spam the admin email address with error messages. The issue is also exploitable via CSRF	6.1	Mo De
CVE-2024-25399	Subrion CMS 4.2.1 is vulnerable to Cross Site Scripting (XSS) via adminer.php.	6.1	Mo De
CVE-2023-7203	The Smart Forms WordPress plugin before 2.6.87 does not have authorisation in various AJAX actions, which could allow users with a role as low as subscriber to call them and perform unauthorised actions such as deleting entries. The plugin also lacks CSRF checks in some places which could allow attackers to make logged in users perform unwanted actions via CSRF attacks such as deleting entries.	6.1	Mo De
CVE-2024-26467	A DOM based cross-site scripting (XSS) vulnerability in the component generator.html of tabatkins/railroad-diagrams before commit ea9a123 allows attackers to execute arbitrary Javascript via sending a crafted URL.	6.1	Mo De
CVE-2023-7167	The Persian Fonts WordPress plugin through 1.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	6.1	Mo De
CVE-2024-26466	A DOM based cross-site scripting (XSS) vulnerability in the component /dom/ranges/Range-test-iframe.html of web-platform-tests/wpt before commit 938e843 allows attackers to execute arbitrary Javascript via sending a crafted URL.	6.1	Mo De
CVE-2024-26465	A DOM based cross-site scripting (XSS) vulnerability in the component /beep/Beep.Instrument.js of stewdio beep.js before commit ef22ad7 allows attackers to execute arbitrary Javascript via sending a crafted URL.	6.1	Mo De
CVE-2024-25875	A cross-site scripting (XSS) vulnerability in the Header module of Enhavo CMS v0.13.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Undertitle text field.	6.1	Mo De
CVE-2024-1810	The Archivist – Custom Archive Templates plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shortcode_attributes' parameter in all versions up to, and including, 1.7.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	Mo De
CVE-2024-25895	A reflected cross-site scripting (XSS) vulnerability in ChurchCRM 5.5.0 allows remote attackers to inject arbitrary web script or HTML via the type parameter of /EventAttendance.php	6.1	Mo De
CVE-2024-26351	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/update_place.php	6.1	Mo De
CVE-2024-26445	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/delete_place.php	6.1	Mo De
CVE-2023-44379	baserCMS is a website development framework. Prior to version 5.0.9, there is a cross-site scripting vulnerability in the site search feature. Version 5.0.9 contains a fix for this vulnerability.	6.1	Mo De
CVE-2024-25876	A cross-site scripting (XSS) vulnerability in the Header module of Enhavo CMS v0.13.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title text field.	6.1	Mo De
CVE-2024-25344	Cross Site Scripting vulnerability in ITFlow.org before commit v.432488eca3998c5be6b6b9e8f8ba01f54bc12378 allows a remtoe attacker to execute arbitrary code and obtain sensitive information via the settings.php, settings+company.php, settings_defaults.php,settings_integrations.php, settings_invoice.php, settings_localization.php, settings_mail.php components.	6.1	Mo De
CVE-2024-26284	Utilizing a 302 redirect, an attacker could have conducted a Universal Cross-Site Scripting (UXSS) on a victim website, if the victim had a link to the attacker's website. This vulnerability affects Focus for iOS < 123.	6.1	Mo De
CVE-2023-38359	IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 260744.	6.1	Mo De
CVE-2024-26491	A cross-site scripting (XSS) vulnerability in the Addon JD Flusity 'Media Gallery with description' module of flusity-CMS v2.33 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Gallery name text field.	6.1	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26484	A stored cross-site scripting (XSS) vulnerability in the Edit Content Layout module of Kirby CMS v4.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Link field. NOTE: the vendor's position is that this issue did not affect any version of Kirby CMS. The only effect was on the trykirby.com demo site, which is not customer-controlled.	6.1	Mo De
CVE-2023-4826	The SocialDriver WordPress theme before version 2024 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties resulting in a cross-site scripting (XSS) attack.	6.1	Mo De
CVE-2024-26148	Querybook is a user interface for querying big data. Prior to version 3.31.1, there is a vulnerability in Querybook's rich text editor that enables users to input arbitrary URLs without undergoing necessary validation. This particular security flaw allows the use of `javascript:` protocol which can potentially trigger arbitrary client-side execution. The most extreme exploit of this flaw could occur when an admin user unknowingly clicks on a cross-site scripting URL, thereby unintentionally compromising admin role access to the attacker. A patch to rectify this issue has been introduced in Querybook version `3.31.1`. The fix is backward compatible and automatically fixes existing DataDocs. There are no known workarounds for this issue, except for manually checking each URL prior to clicking on them.	6.1	Mo De
CVE-2024-25381	There is a Stored XSS Vulnerability in Emlog Pro 2.2.8 Article Publishing, due to non-filtering of quoted content.	6.1	Mo De
CVE-2021-33142	Improper input validation in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow a privileged user to potentially enable denial of service via local access.	6.0	Mo De
CVE-2024-27350	Amazon Fire OS 7 before 7.6.6.9 and 8 before 8.1.0.3 allows Fire TV applications to establish local ADB (Android Debug Bridge) connections. NOTE: some third parties dispute whether this has security relevance, because an ADB connection is only possible after the (non-default) ADB Debugging option is enabled, and after the initiator of that specific connection attempt has been approved via a full-screen prompt.	5.9	Mo De
CVE-2024-26578	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Answer.This issue affects Apache Answer: through 1.2.1. Repeated submission during registration resulted in the registration of the same user. When users register, if they rapidly submit multiple registrations using scripts, it can result in the creation of multiple user accounts simultaneously with the same name. Users are recommended to upgrade to version [1.2.5], which fixes the issue.	5.9	Mo De
CVE-2024-25841	In the module "So Flexibilite" (soflexibilite) from Common-Services for PrestaShop < 4.1.26, a guest (authenticated customer) can perform Cross Site Scripting (XSS) injection.	5.9	Mo De
CVE-2024-26311	Archer Platform 6.x before 6.14 P2 HF1 (6.14.0.2.1) contains a reflected XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this by tricking a victim application user into supplying malicious JavaScript code to the vulnerable web application. This code is then reflected to the victim and gets executed by the web browser in the context of the vulnerable web application.	5.7	Mo De
CVE-2024-1705	A vulnerability was found in Shopwind up to 4.6. It has been rated as critical. This issue affects the function actionCreate of the file /public/install/controllers/DefaultController.php of the component Installation. The manipulation leads to code injection. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-254393 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.6	Mo De
CVE-2024-1920	A vulnerability, which was classified as critical, has been found in osuuu LightPicture up to 1.2.2. This issue affects the function handle of the file /app/middleware/TokenVerify.php. The manipulation leads to use of hard-coded cryptographic key . The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254855.	5.6	Mo De
CVE-2023-51450	baserCMS is a website development framework. Prior to version 5.0.9, there is an OS Command Injection vulnerability in the site search feature of baserCMS. Version 5.0.9 contains a fix for this vulnerability.	5.6	Mo De
CVE-2024-1750	A vulnerability, which was classified as critical, was found in TemmokuMVC up to 2.3. Affected is the function get_img_url/img_replace in the library lib/images_get_down.php of the component Image Download Handler. The manipulation leads to deserialization. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254532. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.6	Mo De
CVE-2024-26602	In the Linux kernel, the following vulnerability has been resolved: sched/membarrier: reduce the ability to hammer on sys_membarrier On some systems, sys_membarrier can be very expensive, causing overall slowdowns for everything. So put a lock on the path in order to serialize the accesses to prevent the ability for this to be called at too high of a frequency and saturate the machine.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46915	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_limit: avoid possible divide error in nft_limit_init div_u64() divides u64 by u32. nft_limit_init() wants to divide u64 by u64, use the appropriate math function (div64_u64) divide error: 0000 [#1] PREEMPT SMP KASAN CPU: 1 PID: 8390 Comm: syz-executor188 Not tainted 5.12.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:div_u64_rem include/linux/math64.h:28 [inline] RIP: 0010:div_u64 include/linux/math64.h:127 [inline] RIP: 0010:nft_limit_init+0x2a2/0x5e0 net/netfilter/nft_limit.c:85 Code: ef 4c 01 eb 41 0f 92 c7 48 89 de e8 38 a5 22 fa 4d 85 ff 0f 85 97 02 00 00 e8 ea 9e 22 fa 4c 0f af f3 45 89 ed 31 d2 4c 89 f0 <49> f7 f5 49 89 c6 e8 d3 9e 22 fa 48 8d 7d 48 48 b8 00 00 00 00 00 RSP: 0018:ffffc90009447198 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000200000000000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffffffff875152e6 RDI: 0000000000000003 RBP: ffff888020f80908 R08: 0000200000000000 R09: 0000000000000000 R10: ffffffff875152d8 R11: 0000000000000000 R12: ffffc90009447270 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 000000000097a300(0000) GS:ffff8880b9d00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000200001c4 CR3: 0000000026a52000 CR4: 00000000001506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: nf_tables_newexpr net/netfilter/nf_tables_api.c:2675 [inline] nft_expr_init+0x145/0x2d0 net/netfilter/nf_tables_api.c:2713 nft_set_elem_expr_alloc+0x27/0x280 net/netfilter/nf_tables_api.c:5160 nf_tables_newset+0x1997/0x3150 net/netfilter/nf_tables_api.c:4321 nfnetlink_rcv_batch+0x85a/0x21b0 net/netfilter/nfnetlink.c:456 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:580 [inline] nfnetlink_rcv+0x3af/0x420 net/netfilter/nfnetlink.c:598 netlink_unicast_kernel net/netlink/af_netlink.c:1312 [inline] netlink_unicast+0x533/0x7d0 net/netlink/af_netlink.c:1338 netlink_sendmsg+0x856/0xd90 net/netlink/af_netlink.c:1927 sock_sendmsg_nosec net/socket.c:654 [inline] sock_sendmsg+0xcf/0x120 net/socket.c:674 ____sys_sendmsg+0x6e8/0x810 net/socket.c:2350 ___sys_sendmsg+0xf3/0x170 net/socket.c:2404 __sys_sendmsg+0xe5/0x1b0 net/socket.c:2433 do_syscall_64+0x2d/0x70 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae	5.5	Mo De
CVE-2021-46927	In the Linux kernel, the following vulnerability has been resolved: nitro_enclaves: Use get_user_pages_unlocked() call to handle mmap assert After commit 5b78ed24e8ec ("mm/pagemap: add mmap_assert_locked() annotations to find_vma*()"), the call to get_user_pages() will trigger the mmap assert. static inline void mmap_assert_locked(struct mm_struct *mm) { lockdep_assert_held(&mm->mmap_lock); VM_BUG_ON_MM(!rwsem_is_locked(&mm->mmap_lock), mm); } [62.521410] kernel BUG at include/linux/mmap_lock.h:156! ..... [62.538938] RIP: 0010:find_vma+0x32/0x80 ..... [62.605889] Call Trace: [62.608502] <TASK> [62.610956] ? lock_timer_base+0x61/0x80 [62.614106] find_extend_vma+0x19/0x80 [62.617195] __get_user_pages+0x9b/0x6a0 [62.620356] __gup_longterm_locked+0x42d/0x450 [62.623721] ? finish_wait+0x41/0x80 [62.626748] ? __kmalloc+0x178/0x2f0 [62.629768] ne_set_user_memory_region_ioctl.isra.0+0x225/0x6a0 [nitro_enclaves] [62.635776] ne_enclave_ioctl+0x1cf/0x6d7 [nitro_enclaves] [62.639541] __x64_sys_ioctl+0x82/0xb0 [62.642620] do_syscall_64+0x3b/0x90 [62.645642] entry_SYSCALL_64_after_hwframe+0x44/0xae Use get_user_pages_unlocked() when setting the enclave memory regions. That's a similar pattern as mmap_read_lock() used together with get_user_pages().	5.5	Mo De
CVE-2021-46914	In the Linux kernel, the following vulnerability has been resolved: ixgbe: fix unbalanced device enable/disable in suspend/resume pci_disable_device() called in __ixgbe_shutdown() decreases dev->enable_cnt by 1. pci_enable_device_mem() which increases dev->enable_cnt by 1, was removed from ixgbe_resume() in commit 6f82b2558735 ("ixgbe: use generic power management"). This caused unbalanced increase/decrease. So add pci_enable_device_mem() back. Fix the following call trace. ixgbe 0000:17:00.1: disabling already-disabled device Call Trace: __ixgbe_shutdown+0x10a/0x1e0 [ixgbe] ixgbe_suspend+0x32/0x70 [ixgbe] pci_pm_suspend+0x87/0x160 ? pci_pm_freeze+0xd0/0xd0 dpm_run_callback+0x42/0x170 __device_suspend+0x114/0x460 async_suspend+0x1f/0xa0 async_run_entry_fn+0x3c/0xf0 process_one_work+0x1dd/0x410 worker_thread+0x34/0x3f0 ? cancel_delayed_work+0x90/0x90 kthread+0x14c/0x170 ? kthread_park+0x90/0x90 ret_from_fork+0x1f/0x30	5.5	Mo De
CVE-2021-46928	In the Linux kernel, the following vulnerability has been resolved: parisc: Clear stale IIR value on instruction access rights trap When a trap 7 (Instruction access rights) occurs, this means the CPU couldn't execute an instruction due to missing execute permissions on the memory region. In this case it seems the CPU didn't even fetched the instruction from memory and thus did not store it in the cr19 (IIR) register before calling the trap handler. So, the trap handler will find some random old stale value in cr19. This patch simply overwrites the stale IIR value with a constant magic "bad food" value (0xbaadf00d), in the hope people don't start to try to understand the various random IIR values in trap 7 dumps.	5.5	Mo De
CVE-2021-46929	In the Linux kernel, the following vulnerability has been resolved: sctp: use call_rcu to free endpoint This patch is to delay the endpoint free by calling call_rcu() to fix another use-after-free issue in sctp_sock_dump(): BUG: KASAN: use-after-free in __lock_acquire+0x36d9/0x4c20 Call Trace: __lock_acquire+0x36d9/0x4c20 kernel/locking/lockdep.c:3218 lock_acquire+0x1ed/0x520 kernel/locking/lockdep.c:3844 __raw_spin_lock_bh include/linux/spinlock_api_smp.h:135 [inline] _raw_spin_lock_bh+0x31/0x40 kernel/locking/spinlock.c:168 spin_lock_bh include/linux/spinlock.h:334 [inline] __lock_sock+0x203/0x350 net/core/sock.c:2253 lock_sock_nested+0xfe/0x120 net/core/sock.c:2774 lock_sock include/net/sock.h:1492 [inline] sctp_sock_dump+0x122/0xb20 net/sctp/diag.c:324 sctp_for_each_transport+0x2b5/0x370 net/sctp/socket.c:5091 sctp_diag_dump+0x3ac/0x660 net/sctp/diag.c:527 __inet_diag_dump+0xa8/0x140 net/ipv4/inet_diag.c:1049 inet_diag_dump+0x9b/0x110 net/ipv4/inet_diag.c:1065 netlink_dump+0x606/0x1080 net/netlink/af_netlink.c:2244 __netlink_dump_start+0x59a/0x7c0 net/netlink/af_netlink.c:2352 netlink_dump_start include/linux/netlink.h:216 [inline] inet_diag_handler_cmd+0x2ce/0x3f0 net/ipv4/inet_diag.c:1170 __sock_diag_cmd net/core/sock_diag.c:232 [inline] sock_diag_rcv_msg+0x31d/0x410 net/core/sock_diag.c:263 netlink_rcv_skb+0x172/0x440 net/netlink/af_netlink.c:2477 sock_diag_rcv+0x2a/0x40 net/core/sock_diag.c:274 This issue occurs when asoc is peeled off and the old sk is freed after getting it by asoc->base.sk and before calling lock_sock(sk). To prevent the sk free, as a holder of the sk, ep should be alive when calling lock_sock(). This patch uses call_rcu() and moves sock_put and ep free into sctp_endpoint_destroy_rcu(), so that it's safe to try to hold the ep under rcu_read_lock in sctp_transport_traverse_process(). If sctp_endpoint_hold() returns true, it means this ep is still alive and we have held it and can continue to dump it; If it returns false, it means this ep is dead and can be freed after rcu_read_unlock, and we should skip it. In sctp_sock_dump(), after locking the sk, if this ep is different from tsp->asoc->ep, it means during this dumping, this asoc was peeled off before calling lock_sock(), and the sk should be skipped; If this ep is the same with tsp->asoc->ep, it means no peeloff happens on this asoc, and due to lock_sock, no peeloff will happen either until release_sock. Note that delaying endpoint free won't delay the port release, as the port release happens in sctp_endpoint_destroy() before calling call_rcu(). Also, freeing endpoint by call_rcu() makes it safe to access the sk by asoc->base.sk in sctp_assocs_seq_show() and sctp_rcv(). Thanks Jones to bring this issue up. v1->v2: - improve the changelog. - add kfree(ep) into sctp_endpoint_destroy_rcu(), as Jakub noticed.	5.5	Mo De
CVE-2021-46930	In the Linux kernel, the following vulnerability has been resolved: usb: mtu3: fix list_head check warning This is caused by uninitialization of list_head. BUG: KASAN: use-after-free in __list_del_entry_valid+0x34/0xe4 Call trace: dump_backtrace+0x0/0x298 show_stack+0x24/0x34 dump_stack+0x130/0x1a8 print_address_description+0x88/0x56c __kasan_report+0x1b8/0x2a0 kasan_report+0x14/0x20 __asan_load8+0x9c/0xa0 __list_del_entry_valid+0x34/0xe4 mtu3_req_complete+0x4c/0x300 [mtu3] mtu3_gadget_stop+0x168/0x448 [mtu3] usb_gadget_unregister_driver+0x204/0x3a0 unregister_gadget_item+0x44/0xa4	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46931	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Wrap the tx reporter dump callback to extract the sq Function mlx5e_tx_reporter_dump_sq() casts its void * argument to struct mlx5e_txqsq *, but in TX-timeout-recovery flow the argument is actually of type struct mlx5e_tx_timeout_ctx *. mlx5_core 0000:08:00.1 enp8s0f1: TX timeout detected mlx5_core 0000:08:00.1 enp8s0f1: TX timeout on queue: 1, SQ: 0x11ec, CQ: 0x146d, SQ Cons: 0x0 SQ Prod: 0x1, usecs since last trans: 21565000 BUG: stack guard page was hit at 0000000093f1a2de (stack is 00000000b66ea0dc..000000004d932dae) kernel stack overflow (page fault): 0000 [#1] SMP NOPTI CPU: 5 PID: 95 Comm: kworker/u20:1 Tainted: G W OE 5.13.0_mlnx #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 Workqueue: mlx5e mlx5e_tx_timeout_work [mlx5_core] RIP: 0010:mlx5e_tx_reporter_dump_sq+0xd3/0x180 [mlx5_core] Call Trace: mlx5e_tx_reporter_dump+0x43/0x1c0 [mlx5_core] devlink_health_do_dump.part.91+0x71/0xd0 devlink_health_report+0x157/0x1b0 mlx5e_reporter_tx_timeout+0xb9/0xf0 [mlx5_core] ? mlx5e_tx_reporter_err_cqe_recover+0x1d0/0x1d0 [mlx5_core] ? mlx5e_health_queue_dump+0xd0/0xd0 [mlx5_core] ? update_load_avg+0x19b/0x550 ? set_next_entity+0x72/0x80 ? pick_next_task_fair+0x227/0x340 ? finish_task_switch+0xa2/0x280 mlx5e_tx_timeout_work+0x83/0xb0 [mlx5_core] process_one_work+0x1de/0x3a0 worker_thread+0x2d/0x3c0 ? process_one_work+0x3a0/0x3a0 kthread+0x115/0x130 ? kthread_park+0x90/0x90 ret_from_fork+0x1f/0x30 --[end trace 51ccabea504edaff]--- RIP: 0010:mlx5e_tx_reporter_dump_sq+0xd3/0x180 PKRU: 55555554 Kernel panic - not syncing: Fatal exception Kernel Offset: disabled end Kernel panic - not syncing: Fatal exception To fix this bug add a wrapper for mlx5e_tx_reporter_dump_sq() which extracts the sq from struct mlx5e_tx_timeout_ctx and set it as the TX-timeout-recovery flow dump callback.	5.5	Mo De
CVE-2023-52467	In the Linux kernel, the following vulnerability has been resolved: mfd: syscon: Fix null pointer dereference in of_syscon_register() kasprintf() returns a pointer to dynamically allocated memory which can be NULL upon failure.	5.5	Mo De
CVE-2024-26601	In the Linux kernel, the following vulnerability has been resolved: ext4: regenerate buddy after block freeing failed if under fc replay This mostly reverts commit 6bd97bf273bd ("ext4: remove redundant mb_regenerate_buddy()") and reintroduces mb_regenerate_buddy(). Based on code in mb_free_blocks(), fast commit replay can end up marking as free blocks that are already marked as such. This causes corruption of the buddy bitmap so we need to regenerate it in that case.	5.5	Mo De
CVE-2021-46926	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: intel-sdw-acpi: harden detection of controller The existing code currently sets a pointer to an ACPI handle before checking that it's actually a SoundWire controller. This can lead to issues where the graph walk continues and eventually fails, but the pointer was set already. This patch changes the logic so that the information provided to the caller is set when a controller is found.	5.5	Mo De
CVE-2021-46932	In the Linux kernel, the following vulnerability has been resolved: Input: appletouch - initialize work before device registration Syzbot has reported warning in __flush_work(). This warning is caused by work->func == NULL, which means missing work initialization. This may happen, since input_dev->close() calls cancel_work_sync(&dev->work), but dev->work initalization happens _after_ input_register_device() call. So this patch moves dev->work initialization before registering input device	5.5	Mo De
CVE-2021-46933	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_fs: Clear ffs_eventfd in ffs_data_clear. ffs_data_clear is indirectly called from both ffs_fs_kill_sb and ffs_ep0_release, so it ends up being called twice when userland closes ep0 and then unmounts f_fs. If userland provided an eventfd along with function's USB descriptors, it ends up calling eventfd_ctx_put as many times, causing a refcount underflow. NULL-ify ffs_eventfd to prevent these extraneous eventfd_ctx_put calls. Also, set epfiles to NULL right after de-allocating it, for readability. For completeness, ffs_data_clear actually ends up being called thrice, the last call being before the whole ffs structure gets freed, so when this specific sequence happens there is a second underflow happening (but not being reported): /sys/kernel/debug/tracing# modprobe usb_f_fs /sys/kernel/debug/tracing# echo ffs_data_clear > set_ftrace_filter /sys/kernel/debug/tracing# echo function > current_tracer /sys/kernel/debug/tracing# echo 1 > tracing_on (setup gadget, run and kill function userland process, teardown gadget) /sys/kernel/debug/tracing# echo 0 > tracing_on /sys/kernel/debug/tracing# cat trace smartcard-openp-436 [000] ..... 1946.208786: ffs_data_clear <-ffs_data_closed smartcard-openp-431 [000] ..... 1946.279147: ffs_data_clear <-ffs_data_closed smartcard-openp-431 [000] .n... 1946.905512: ffs_data_clear <-ffs_data_put Warning output corresponding to above trace: [1946.284139] WARNING: CPU: 0 PID: 431 at lib/refcount.c:28 refcount_warn_saturate+0x110/0x15c [1946.293094] refcount_t: underflow; use-after-free. [1946.298164] Modules linked in: usb_f_ncm(E) u_ether(E) usb_f_fs(E) hci_uart(E) btqca(E) btrtl(E) btbcm(E) btintel(E) bluetooth(E) nls_ascii(E) nls_cp437(E) vfat(E) fat(E) bcm2835_v4l2(CE) bcm2835_mmal_vchiq(CE) videobuf2_vmalloc(E) videobuf2_memops(E) sha512_generic(E) videobuf2_v4l2(E) sha512_arm(E) videobuf2_common(E) videodev(E) cpufreq_dt(E) snd_bcm2835(CE) brcmfmac(E) mc(E) vc4(E) ctr(E) brcmutil(E) snd_soc_core(E) snd_pcm_dmaengine(E) drbg(E) snd_pcm(E) snd_timer(E) snd(E) soundcore(E) drm_kms_helper(E) cec(E) ansi_cprng(E) rc_core(E) syscopyarea(E) raspberrypi_cpufreq(E) sysfillrect(E) sysimgblt(E) cfg80211(E) max17040_battery(OE) raspberrypi_hwmon(E) fb_sys_fops(E) regmap_i2c(E) ecdh_generic(E) rfkill(E) ecc(E) bcm2835_rng(E) rng_core(E) vchiq(CE) leds_gpio(E) libcomposite(E) fuse(E) configfs(E) ip_tables(E) x_tables(E) autofs4(E) ext4(E) crc16(E) mbcache(E) jbd2(E) crc32c_generic(E) sdhci_iproc(E) sdhci_pltfm(E) sdhci(E) [1946.399633] CPU: 0 PID: 431 Comm: smartcard-openp Tainted: G C OE 5.15.0-1-rpi #1 Debian 5.15.3-1 [1946.417950] Hardware name: BCM2835 [1946.425442] Backtrace: [1946.432048] [<c08d60a0>] (dump_backtrace) from [<c08d62ec>] (show_stack+0x20/0x24) [1946.448226] r7:00000009 r6:0000001c r5:c04a948c r4:c0a64e2c [1946.458412] [<c08d62cc>] (show_stack) from [<c08d9ae0>] (dump_stack+0x28/0x30) [1946.470380] [<c08d9ab8>] (dump_stack) from [<c0123500>] (__warn+0xe8/0x154) [1946.482067] r5:c04a948c r4:c0a71dc8 [1946.490184] [<c0123418>] (__warn) from [<c08d6948>] (warn_slowpath_fmt+0xa0/0xe4) [1946.506758] r7:00000009 r6:0000001c r5:c0a71dc8 r4:c0a71e04 [1946.517070] [<c08d68ac>] (warn_slowpath_fmt) from [<c04a948c>] (refcount_warn_saturate+0x110/0x15c) [1946.535309] r8:c0100224 r7:c0dfcb84 r6:ffffffff r5:c3b84c00 r4:c24a17c0 [1946.546708] [<c04a937c>] (refcount_warn_saturate) from [<c0380134>] (eventfd_ctx_put+0x48/0x74) [1946.564476] [<c03800ec>] (eventfd_ctx_put) from [<bf5464e8>] (ffs_data_clear+0xd0/0x118 [usb_f_fs]) [1946.582664] r5:c3b84c00 r4:c2695b00 [1946.590668] [<bf546418>] (ffs_data_clear [usb_f_fs]) from [<bf547cc0>] (ffs_data_closed+0x9c/0x150 [usb_f_fs]) [1946.609608] r5:bf54d014 r4:c2695b00 [1946.617522] [<bf547c24>] (ffs_data_closed [usb_f_fs]) from [<bf547da0>] (ffs_fs_kill_sb+0x2c/0x30 [usb_f_fs]) [1946.636217] r7:c0dfcb ---truncated---	5.5	Mo De
CVE-2021-46912	In the Linux kernel, the following vulnerability has been resolved: net: Make tcp_allowed_congestion_control readonly in non-init netns Currently, tcp_allowed_congestion_control is global and writable; writing to it in any net namespace will leak into all other net namespaces. tcp_available_congestion_control and tcp_allowed_congestion_control are the only sysctls in ipv4_net_table (the per-netns sysctl table) with a NULL data pointer; their handlers (proc_tcp_available_congestion_control and proc_allowed_congestion_control) have no other way of referencing a struct net. Thus, they operate globally. Because ipv4_net_table does not use designated initializers, there is no easy way to fix up this one "bad" table entry. However, the data pointer updating logic shouldn't be applied to NULL pointers anyway, so we instead force these entries to be read-only. These sysctls used to exist in ipv4_table (init-net only), but they were moved to the per-net ipv4_net_table, presumably without realizing that tcp_allowed_congestion_control was writable and thus introduced a leak. Because the intent of that commit was only to know (i.e. read) "which congestion algorithms are available or allowed", this read-only solution should be sufficient. The logic added in recent commit 31c4d2f160eb: ("net: Ensure net namespace isolation of sysctls") does not and cannot check for NULL data pointers, because other table entries (e.g. /proc/sys/net/netfilter/nf_log/) have .data=NULL but use other methods (.extra2) to access the struct net.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46935	In the Linux kernel, the following vulnerability has been resolved: binder: fix async_free_space accounting for empty parcels In 4.13, commit 74310e06be4d ("android: binder: Move buffer out of area shared with user space") fixed a kernel structure visibility issue. As part of that patch, sizeof(void *) was used as the buffer size for 0-length data payloads so the driver could detect abusive clients sending 0-length asynchronous transactions to a server by enforcing limits on async_free_size. Unfortunately, on the "free" side, the accounting of async_free_space did not add the sizeof(void *) back. The result was that up to 8-bytes of async_free_space were leaked on every async transaction of 8-bytes or less. These small transactions are uncommon, so this accounting issue has gone undetected for several years. The fix is to use "buffer_size" (the allocated buffer size) instead of "size" (the logical buffer size) when updating the async_free_space during the free operation. These are the same except for this corner case of asynchronous transactions with payloads < 8 bytes.	5.5	Mo De
CVE-2021-46913	In the Linux kernel, the following vulnerability has been resolved: netfilter: nftables: clone set element expression template memcpy() breaks when using connlimit in set elements. Use nft_expr_clone() to initialize the connlimit expression list, otherwise connlimit garbage collector crashes when walking on the list head copy. [493.064656] Workqueue: events_power_efficient nft_rhash_gc [nf_tables] [493.064685] RIP: 0010:find_or_evict+0x5a/0x90 [nf_conncount] [493.064694] Code: 2b 43 40 83 f8 01 77 0d 48 c7 c0 f5 ff ff ff 44 39 63 3c 75 df 83 6d 18 01 48 8b 43 08 48 89 de 48 8b 13 48 8b 3d ee 2f 00 00 <48> 89 42 08 48 89 10 48 b8 00 01 00 00 00 00 ad de 48 89 03 48 83 [493.064699] RSP: 0018:ffffc90000417dc0 EFLAGS: 00010297 [493.064704] RAX: 0000000000000000 RBX: ffff888134f38410 RCX: 0000000000000000 [493.064708] RDX: 0000000000000000 RSI: ffff888134f38410 RDI: ffff888100060cc0 [493.064711] RBP: ffff88812ce594a8 R08: ffff888134f38438 R09: 00000000ebb9025c [493.064714] R10: ffffffff8219f838 R11: 0000000000000017 R12: 0000000000000001 [493.064718] R13: ffffffff82146740 R14: ffff888134f38410 R15: 0000000000000000 [493.064721] FS: 0000000000000000(0000) GS:ffff88840e440000(0000) knlGS:0000000000000000 [493.064725] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [493.064729] CR2: 0000000000000008 CR3: 00000001330aa002 CR4: 00000000001706e0 [493.064733] Call Trace: [493.064737] nf_conncount_gc_list+0x8f/0x150 [nf_conncount] [493.064746] nft_rhash_gc+0x106/0x390 [nf_tables]	5.5	Mo De
CVE-2021-46909	In the Linux kernel, the following vulnerability has been resolved: ARM: footbridge: fix PCI interrupt mapping Since commit 30fdfb929e82 ("PCI: Add a call to pci_assign_irq() in pci_device_probe()"), the PCI code will call the IRQ mapping function whenever a PCI driver is probed. If these are marked as __init, this causes an oops if a PCI driver is loaded or bound after the kernel has initialised.	5.5	Mo De
CVE-2021-46905	In the Linux kernel, the following vulnerability has been resolved: net: hso: fix NULL-deref on disconnect regression Commit 8a12f8836145 ("net: hso: fix null-ptr-deref during tty device unregistration") fixed the racy minor allocation reported by syzbot, but introduced an unconditional NULL-pointer dereference on every disconnect instead. Specifically, the serial device table must no longer be accessed after the minor has been released by hso_serial_tty_unregister().	5.5	Mo De
CVE-2021-46904	In the Linux kernel, the following vulnerability has been resolved: net: hso: fix null-ptr-deref during tty device unregistration Multiple ttys try to claim the same the minor number causing a double unregistration of the same device. The first unregistration succeeds but the next one results in a null-ptr-deref. The get_free_serial_index() function returns an available minor number but doesn't assign it immediately. The assignment is done by the caller later. But before this assignment, calls to get_free_serial_index() would return the same minor number. Fix this by modifying get_free_serial_index to assign the minor number immediately after one is found to be and rename it to obtain_minor() to better reflect what it does. Similary, rename set_serial_by_index() to release_minor() and modify it to free up the minor number of the given hso_serial. Every obtain_minor() should have corresponding release_minor() call.	5.5	Mo De
CVE-2024-26600	In the Linux kernel, the following vulnerability has been resolved: phy: ti: phy-omap-usb2: Fix NULL pointer dereference for SRP If the external phy working together with phy-omap-usb2 does not implement send_srp(), we may still attempt to call it. This can happen on an idle Ethernet gadget triggering a wakeup for example: configfs-gadget.g1 gadget.0: ECM Suspend configfs-gadget.g1 gadget.0: Port suspended. Triggering wakeup ... Unable to handle kernel NULL pointer dereference at virtual address 00000000 when execute ... PC is at 0x0 LR is at musb_gadget_wakeup+0x1d4/0x254 [musb_hdrc] ... musb_gadget_wakeup [musb_hdrc] from usb_gadget_wakeup+0x1c/0x3c [udc_core] usb_gadget_wakeup [udc_core] from eth_start_xmit+0x3b0/0x3d4 [u_ether] eth_start_xmit [u_ether] from dev_hard_start_xmit+0x94/0x24c dev_hard_start_xmit from sch_direct_xmit+0x104/0x2e4 sch_direct_xmit from __dev_queue_xmit+0x334/0xd88 __dev_queue_xmit from arp_solicit+0xf0/0x268 arp_solicit from neigh_probe+0x54/0x7c neigh_probe from __neigh_event_send+0x22c/0x47c __neigh_event_send from neigh_resolve_output+0x14c/0x1c0 neigh_resolve_output from ip_finish_output2+0x1c8/0x628 ip_finish_output2 from ip_send_skb+0x40/0xd8 ip_send_skb from udp_send_skb+0x124/0x340 udp_send_skb from udp_sendmsg+0x780/0x984 udp_sendmsg from __sys_sendto+0xd8/0x158 __sys_sendto from ret_fast_syscall+0x0/0x58 Let's fix the issue by checking for send_srp() and set_vbus() before calling them. For USB peripheral only cases these both could be NULL.	5.5	Mo De
CVE-2020-36775	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid potential deadlock Using f2fs_trylock_op() in f2fs_write_compressed_pages() to avoid potential deadlock like we did in f2fs_write_single_data_page().	5.5	Mo De
CVE-2021-46906	In the Linux kernel, the following vulnerability has been resolved: HID: usbhid: fix info leak in hid_submit_ctrl In hid_submit_ctrl(), the way of calculating the report length doesn't take into account that report->size can be zero. When running the syzkaller reproducer, a report of size 0 causes hid_submit_ctrl) to calculate transfer_buffer_length as 16384. When this urb is passed to the usb core layer, KMSAN reports an info leak of 16384 bytes. To fix this, first modify hid_report_len() to account for the zero report size case by using DIV_ROUND_UP for the division. Then, call it from hid_submit_ctrl().	5.5	Mo De
CVE-2021-46922	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: Fix TPM reservation for seal/unseal The original patch 8c657a0590de ("KEYS: trusted: Reserve TPM for seal and unseal operations") was correct on the mailing list: https://lore.kernel.org/linux-integrity/20210128235621.127925-4-jarkko@kernel.org/ But somehow got rebased so that the tpm_try_get_ops() in tpm2_seal_trusted() got lost. This causes an imbalanced put of the TPM ops and causes oopses on TIS based hardware. This fix puts back the lost tpm_try_get_ops()	5.5	Mo De
CVE-2024-26604	In the Linux kernel, the following vulnerability has been resolved: Revert "kobject: Remove redundant checks for whether ktype is NULL" This reverts commit 1b28cb81dab7c1eedc6034206f4e8d644046ad31. It is reported to cause problems, so revert it for now until the root cause can be found.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46910	In the Linux kernel, the following vulnerability has been resolved: ARM: 9063/1: mm: reduce maximum number of CPUs if DEBUG_KMAP_LOCAL is enabled The debugging code for kmap_local() doubles the number of per-CPU fixmap slots allocated for kmap_local(), in order to use half of them as guard regions. This causes the fixmap region to grow downwards beyond the start of its reserved window if the supported number of CPUs is large, and collide with the newly added virtual DT mapping right below it, which is obviously not good. One manifestation of this is EFI boot on a kernel built with NR_CPUS=32 and CONFIG_DEBUG_KMAP_LOCAL=y, which may pass the FDT in highmem, resulting in block entries below the fixmap region that the fixmap code misidentifies as fixmap table entries, and subsequently tries to dereference using a phys-to-virt translation that is only valid for lowmem. This results in a cryptic splat such as the one below. ftrace: allocating 45548 entries in 89 pages 8<--- cut here --- Unable to handle kernel paging request at virtual address fc6006f0 pgd = (ptrval) [fc6006f0] *pgd=80000040207003, *pmd=00000000 Internal error: Oops: a06 [#1] SMP ARM Modules linked in: CPU: 0 PID: 0 Comm: swapper Not tainted 5.11.0+ #382 Hardware name: Generic DT based system PC is at cpu_ca15_set_pte_ext+0x24/0x30 LR is at __set_fixmap+0xe4/0x118 pc : [<c041ac9c>] lr : [<c04189d8>] psr: 400000d3 sp : c1601ed8 ip : 00400000 fp : 00800000 r10: 0000071f r9 : 00421000 r8 : 00c00000 r7 : 00c00000 r6 : 0000071f r5 : ffade000 r4 : 4040171f r3 : 00c00000 r2 : 4040171f r1 : c041ac78 r0 : fc6006f0 Flags: nZcv IRQs off FIQs off Mode SVC_32 ISA ARM Segment none Control: 30c5387d Table: 40203000 DAC: 00000001 Process swapper (pid: 0, stack limit = 0x(ptrval)) So let's limit CONFIG_NR_CPUS to 16 when CONFIG_DEBUG_KMAP_LOCAL=y. Also, fix the BUILD_BUG_ON() check that was supposed to catch this, by checking whether the region grows below the start address rather than above the end address.	5.5	Mo De
CVE-2021-46911	In the Linux kernel, the following vulnerability has been resolved: ch_ktls: Fix kernel panic Taking page refcount is not ideal and causes kernel panic sometimes. It's better to take tx_ctx lock for the complete skb transmit, to avoid page cleanup if ACK received in middle.	5.5	Mo De
CVE-2023-52470	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: check the alloc_workqueue return value in radeon_crtc_init() check the alloc_workqueue return value in radeon_crtc_init() to avoid null-ptr-deref.	5.5	Mo De
CVE-2024-26605	In the Linux kernel, the following vulnerability has been resolved: PCI/ASPM: Fix deadlock when enabling ASPM A last minute revert in 6.7-final introduced a potential deadlock when enabling ASPM during probe of Qualcomm PCIe controllers as reported by lockdep: == WARNING: possible recursive locking detected 6.7.0 #40 Not tainted -- kworker/u16:5/90 is trying to acquire lock: ffffacfa78ced000 (pci_bus_sem){++++}-{3:3}, at: pcie_aspm_pm_state_change+0x58/0xdc but task is already holding lock: ffffacfa78ced000 (pci_bus_sem){++++}-{3:3}, at: pci_walk_bus+0x34/0xbc other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(pci_bus_sem); lock(pci_bus_sem); *** DEADLOCK *** Call trace: print_deadlock_bug+0x25c/0x348 __lock_acquire+0x10a4/0x2064 lock_acquire+0x1e8/0x318 down_read+0x60/0x184 pcie_aspm_pm_state_change+0x58/0xdc pci_set_full_power_state+0xa8/0x114 pci_set_power_state+0xc4/0x120 qcom_pcie_enable_aspm+0x1c/0x3c [pcie_qcom] pci_walk_bus+0x64/0xbc qcom_pcie_host_post_init_2_7_0+0x28/0x34 [pcie_qcom] The deadlock can easily be reproduced on machines like the Lenovo ThinkPad X13s by adding a delay to increase the race window during asynchronous probe where another thread can take a write lock. Add a new pci_set_power_state_locked() and associated helper functions that can be called with the PCI bus semaphore held to avoid taking the read lock twice.	5.5	Mo De
CVE-2021-46921	In the Linux kernel, the following vulnerability has been resolved: locking/qrwlock: Fix ordering in queued_write_lock_slowpath() While this code is executed with the wait_lock held, a reader can acquire the lock without holding wait_lock. The writer side loops checking the value with the atomic_cond_read_acquire(), but only truly acquires the lock when the compare-and-exchange is completed successfully which isn't ordered. This exposes the window between the acquire and the cmpxchg to an A-B-A problem which allows reads following the lock acquisition to observe values speculatively before the write lock is truly acquired. We've seen a problem in epoll where the reader does a xchg while holding the read lock, but the writer can see a value change out from under it. Writer I Reader ---------- ep_scan_ready_list() I I-write_lock_irq() I I- queued_write_lock_slowpath() I I- atomic_cond_read_acquire() I I read_lock_irqsave(&ep->lock, flags); --> (observes value before unlock) I chain_epi_lockless() I I epi->next = xchg(&ep->ovflist, epi); I I read_unlock_irqrestore(&ep->lock, flags); I I I atomic_cmpxchg_relaxed() I I-- READ_ONCE(ep->ovflist); I A core can order the read of the ovflist ahead of the atomic_cmpxchg_relaxed(). Switching the cmpxchg to use acquire semantics addresses this issue at which point the atomic_cond_read can be switched to use relaxed semantics. [peterz: use try_cmpxchg()]	5.5	Mo De
CVE-2024-26606	In the Linux kernel, the following vulnerability has been resolved: binder: signal epoll threads of self-work In (e)poll mode, threads often depend on I/O events to determine when data is ready for consumption. Within binder, a thread may initiate a command via BINDER_WRITE_READ without a read buffer and then make use of epoll_wait() or similar to consume any responses afterwards. It is then crucial that epoll threads are signaled via wakeup when they queue their own work. Otherwise, they risk waiting indefinitely for an event leaving their work unhandled. What is worse, subsequent commands won't trigger a wakeup either as the thread has pending work.	5.5	Mo De
CVE-2023-52465	In the Linux kernel, the following vulnerability has been resolved: power: supply: Fix null pointer dereference in smb2_probe devm_kasprintf and devm_kzalloc return a pointer to dynamically allocated memory which can be NULL upon failure.	5.5	Mo De
CVE-2023-52471	In the Linux kernel, the following vulnerability has been resolved: ice: Fix some null pointer dereference issues in ice_ptp.c devm_kasprintf() returns a pointer to dynamically allocated memory which can be NULL upon failure.	5.5	Mo De
CVE-2021-46923	In the Linux kernel, the following vulnerability has been resolved: fs/mount_setattr: always cleanup mount_kattr Make sure that finish_mount_kattr() is called after mount_kattr was succesfully built in both the success and failure case to prevent leaking any references we took when we built it. We returned early if path lookup failed thereby risking to leak an additional reference we took when building mount_kattr when an idmapped mount was requested.	5.5	Mo De
CVE-2021-46916	In the Linux kernel, the following vulnerability has been resolved: ixgbe: Fix NULL pointer dereference in ethtool loopback test The ixgbe driver currently generates a NULL pointer dereference when performing the ethtool loopback test. This is due to the fact that there isn't a q_vector associated with the test ring when it is setup as interrupts are not normally added to the test rings. To address this I have added code that will check for a q_vector before returning a napi_id value. If a q_vector is not present it will return a value of 0.	5.5	Mo De
CVE-2023-52472	In the Linux kernel, the following vulnerability has been resolved: crypto: rsa - add a check for allocation failure Static checkers insist that the mpi_alloc() allocation can fail so add a check to prevent a NULL dereference. Small allocations like this can't actually fail in current kernels, but adding a check is very simple and makes the static checkers happy.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-25763	openNDS 10.2.0 is vulnerable to Use-After-Free via /openNDS/src/auth.c.	5.5	Mo De
CVE-2023-52473	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Fix NULL pointer dereference in zone registration error path If device_register() in thermal_zone_device_register_with_trips() returns an error, the tz variable is set to NULL and subsequently dereferenced in kfree(tz->tzp). Commit adc8749b150c ("thermal/drivers/core: Use put_device() if device_register() fails") added the tz = NULL assignment in question to avoid a possible double-free after dropping the reference to the zone device. However, after commit 4649620d9404 ("thermal: core: Make thermal_zone_device_unregister() return after freeing the zone"), that assignment has become redundant, because dropping the reference to the zone device does not cause the zone object to be freed any more. Drop it to address the NULL pointer dereference.	5.5	Mo De
CVE-2024-26603	In the Linux kernel, the following vulnerability has been resolved: x86/fpu: Stop relying on userspace for info to fault in xsave buffer Before this change, the expected size of the user space buffer was taken from fx_sw->xstate_size. fx_sw->xstate_size can be changed from user-space, so it is possible construct a sigreturn frame where: * fx_sw->xstate_size is smaller than the size required by valid bits in fx_sw->xfeatures. * user-space unmaps parts of the sigrame fpu buffer so that not all of the buffer required by xrstor is accessible. In this case, xrstor tries to restore and accesses the unmapped area which results in a fault. But fault_in_readable succeeds because buf + fx_sw->xstate_size is within the still mapped area, so it goes back and tries xrstor again. It will spin in this loop forever. Instead, fault in the maximum size which can be touched by XRSTOR (taken from fpstate->user_size). [dhansen: tweak subject / changelog]	5.5	Mo De
CVE-2021-46924	In the Linux kernel, the following vulnerability has been resolved: NFC: st21nfca: Fix memory leak in device probe and remove 'phy->pending_skb' is alloced when device probe, but forgot to free in the error handling path and remove path, this cause memory leak as follows: unreferenced object 0xffff88800bc06800 (size 512): comm "8", pid 11775, jiffies 4295159829 (age 9.032s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<00000000d66c09ce>] __kmalloc_node_track_caller+0x1ed/0x450 [<00000000c93382b3>] kmalloc_reserve+0x37/0xd0 [<000000005fea522c>] __alloc_skb+0x124/0x380 [<0000000019f29f9a>] st21nfca_hci_i2c_probe+0x170/0x8f2 Fix it by freeing 'pending_skb' in error and remove.	5.5	Mo De
CVE-2021-46920	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix clobbering of SWERR overflow bit on writeback Current code blindly writes over the SWERR and the OVERFLOW bits. Write back the bits actually read instead so the driver avoids clobbering the OVERFLOW bit that comes after the register is read.	5.5	Mo De
CVE-2021-46919	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix wq size store permission state WQ size can only be changed when the device is disabled. Current code allows change when device is enabled but wq is disabled. Change the check to detect device state.	5.5	Mo De
CVE-2021-46918	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: clear MSIX permission entry on shutdown Add disabling/clearing of MSIX permission entries on device shutdown to mirror the enabling of the MSIX entries on probe. Current code left the MSIX enabled and the pasid entries still programmed at device shutdown.	5.5	Mo De
CVE-2021-46917	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix wq cleanup of WQCFG registers A pre-release silicon erratum workaround where wq reset does not clear WQCFG registers was leaked into upstream code. Use wq reset command instead of blasting the MMIO region. This also address an issue where we clobber registers in future devices.	5.5	Mo De
CVE-2021-46908	In the Linux kernel, the following vulnerability has been resolved: bpf: Use correct permission flag for mixed signed bounds arithmetic We forbid adding unknown scalars with mixed signed bounds due to the spectre v1 masking mitigation. Hence this also needs bypass_spec_v1 flag instead of allow_ptr_leaks.	5.5	Mo De
CVE-2020-36777	In the Linux kernel, the following vulnerability has been resolved: media: dvbdev: Fix memory leak in dvb_media_device_free() dvb_media_device_free() is leaking memory. Free `dvbdev->adapter->conn` before setting it to NULL, as documented in include/media/media-device.h: "The media_entity instance itself must be freed explicitly by the driver if required."	5.5	Mo De
CVE-2021-46937	In the Linux kernel, the following vulnerability has been resolved: mm/damon/dbgfs: fix 'struct pid' leaks in 'dbgfs_target_ids_write()' DAMON debugfs interface increases the reference counts of 'struct pid's for targets from the 'target_ids' file write callback ('dbgfs_target_ids_write()'), but decreases the counts only in DAMON monitoring termination callback ('dbgfs_before_terminate()'). Therefore, when 'target_ids' file is repeatedly written without DAMON monitoring start/termination, the reference count is not decreased and therefore memory for the 'struct pid' cannot be freed. This commit fixes this issue by decreasing the reference counts when 'target_ids' is written.	5.5	Mo De
CVE-2023-52443	In the Linux kernel, the following vulnerability has been resolved: apparmor: avoid crash when parsed profile name is empty When processing a packed profile in unpack_profile() described like "profile :ns::samba-dcerpcd /usr/lib*/samba/{,samba/}samba-dcerpcd {...}" a string ":samba-dcerpcd" is unpacked as a fully-qualified name and then passed to aa_splitn_fqname(). aa_splitn_fqname() treats ":samba-dcerpcd" as only containing a namespace. Thus it returns NULL for tmpname, meanwhile tmpns is non-NULL. Later aa_alloc_profile() crashes as the new profile name is NULL now. general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] PREEMPT SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 6 PID: 1657 Comm: apparmor_parser Not tainted 6.7.0-rc2-dirty #16 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 RIP: 0010:strlen+0x1e/0xa0 Call Trace: <TASK> ? strlen+0x1e/0xa0 aa_policy_init+0x1bb/0x230 aa_alloc_profile+0xb1/0x480 unpack_profile+0x3bc/0x4960 aa_unpack+0x309/0x15e0 aa_replace_profiles+0x213/0x33c0 policy_update+0x261/0x370 profile_replace+0x20e/0x2a0 vfs_write+0x2af/0xe00 ksys_write+0x126/0x250 do_syscall_64+0x46/0xf0 entry_SYSCALL_64_after_hwframe+0x6e/0x76 </TASK> ---[end trace 0000000000000000]--- RIP: 0010:strlen+0x1e/0xa0 It seems such behaviour of aa_splitn_fqname() is expected and checked in other places where it is called (e.g. aa_remove_profiles). Well, there is an explicit comment "a ns name without a following profile is allowed" inside. AFAICS, nothing can prevent unpacked "name" to be in form like ":samba-dcerpcd" - it is passed from userspace. Deny the whole profile set replacement in such case and inform user with EPROTO and an explaining message. Found by Linux Verification Center (linuxtesting.org).	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46960	In the Linux kernel, the following vulnerability has been resolved: cifs: Return correct error code from smb2_get_enc_key Avoid a warning if the error percolates back up: [440700.376476] CIFS VFS: \\otters.example.com crypt_message: Could not get encryption key [440700.386947] ------------[cut here]------------ [440700.386948] err = 1 [440700.386977] WARNING: CPU: 11 PID: 2733 at /build/linux-hwe-5.4-p6lk6L/linux-hwe-5.4-5.4.0/lib/errseq.c:74 errseq_set+0x5c/0x70 ... [440700.397304] CPU: 11 PID: 2733 Comm: tar Tainted: G OE 5.4.0-70-generic #78~18.04.1-Ubuntu ... [440700.397334] Call Trace: [440700.397346] __filemap_set_wb_err+0x1a/0x70 [440700.397419] cifs_writepages+0x9c7/0xb30 [cifs] [440700.397426] do_writepages+0x4b/0xe0 [440700.397444] __filemap_fdatawrite_range+0xcb/0x100 [440700.397455] filemap_write_and_wait+0x42/0xa0 [440700.397486] cifs_setattr+0x68b/0xf30 [cifs] [440700.397493] notify_change+0x358/0x4a0 [440700.397500] utimes_common+0xe9/0x1c0 [440700.397510] do_utimes+0xc5/0x150 [440700.397520] __x64_sys_utimensat+0x88/0xd0	5.5	Mo De
CVE-2021-46957	In the Linux kernel, the following vulnerability has been resolved: riscv/kprobe: fix kernel panic when invoking sys_read traced by kprobe The execution of sys_read end up hitting a BUG_ON() in __find_get_block after installing kprobe at sys_read, the BUG message like the following: [65.708663] ------------[cut here]------------ [65.709987] kernel BUG at fs/buffer.c:1251! [65.711283] Kernel BUG [#1] [65.712032] Modules linked in: [65.712925] CPU: 0 PID: 51 Comm: sh Not tainted 5.12.0-rc4 #1 [65.714407] Hardware name: riscv-virtio,qemu (DT) [65.715696] epc : __find_get_block+0x218/0x2c8 [65.716835] ra : __getblk_gfp+0x1c/0x4a [65.717831] epc : ffffffe00019f11e ra : ffffffe00019f56a sp : ffffffe002437930 [65.719553] gp : ffffffe000f06030 tp : ffffffe0015abc00 t0 : ffffffe00191e038 [65.721290] t1 : ffffffe00191e038 t2 : 000000000000000a s0 : ffffffe002437960 [65.723051] s1 : ffffffe00160ad00 a0 : ffffffe00160ad00 a1 : 000000000000012a [65.724772] a2 : 0000000000000400 a3 : 0000000000000008 a4 : 0000000000000040 [65.726545] a5 : 0000000000000000 a6 : ffffffe00191e000 a7 : 0000000000000000 [65.728308] s2 : 000000000000012a s3 : 0000000000000400 s4 : 0000000000000008 [65.730049] s5 : 000000000000006c s6 : ffffffe00240f800 s7 : ffffffe000f080a8 [65.731802] s8 : 0000000000000001 s9 : 000000000000012a s10: 0000000000000008 [65.733516] s11: 0000000000000008 t3 : 00000000000003ff t4 : 000000000000000f [65.734434] t5 : 00000000000003ff t6 : 0000000000040000 [65.734613] status: 0000000000000100 badaddr: 0000000000000000 cause: 0000000000000003 [65.734901] Call Trace: [65.735076] [<ffffffe00019f11e>] __find_get_block+0x218/0x2c8 [65.735417] [<ffffffe00020017a>] __ext4_get_inode_loc+0xb2/0x2f6 [65.735618] [<ffffffe000201b6c>] ext4_get_inode_loc+0x3a/0x8a [65.735802] [<ffffffe000203380>] ext4_reserve_inode_write+0x2e/0x8c [65.735999] [<ffffffe00020357a>] __ext4_mark_inode_dirty+0x4c/0x18e [65.736208] [<ffffffe000206bb0>] ext4_dirty_inode+0x46/0x66 [65.736387] [<ffffffe000192914>] __mark_inode_dirty+0x12c/0x3da [65.736576] [<ffffffe000180dd2>] touch_atime+0x146/0x150 [65.736748] [<ffffffe00010d762>] filemap_read+0x234/0x246 [65.736920] [<ffffffe00010d834>] generic_file_read_iter+0xc0/0x114 [65.737114] [<ffffffe0001f5d7a>] ext4_file_read_iter+0x42/0xea [65.737310] [<ffffffe000163f2c>] new_sync_read+0xe2/0x15a [65.737483] [<ffffffe000165814>] vfs_read+0xca/0xf2 [65.737641] [<ffffffe000165bae>] ksys_read+0x5e/0xc8 [65.737816] [<ffffffe000165c26>] sys_read+0xe/0x16 [65.737973] [<ffffffe000003972>] ret_from_syscall+0x0/0x2 [65.738858] ---[end trace fe93f985456c935d]--- A simple reproducer looks like: echo 'p:myprobe sys_read fd=%a0 buf=%a1 count=%a2' > /sys/kernel/debug/tracing/kprobe_events echo 1 > /sys/kernel/debug/tracing/events/kprobes/myprobe/enable cat /sys/kernel/debug/tracing/trace Here's what happens to hit that BUG_ON(): 1) After installing kprobe at entry of sys_read, the first instruction is replaced by 'ebreak' instruction on riscv64 platform. 2) Once kernel reach the 'ebreak' instruction at the entry of sys_read, it trap into the riscv breakpoint handler, where it do something to setup for coming single-step of origin instruction, including backup the 'sstatus' in pt_regs, followed by disable interrupt during single stepping via clear 'SIE' bit of 'sstatus' in pt_regs. 3) Then kernel restore to the instruction slot contains two instructions, one is original instruction at entry of sys_read, the other is 'ebreak'. Here it trigger a 'Instruction page fault' exception (value at 'scause' is '0xc'), if PF is not filled into PageTabe for that slot yet. 4) Again kernel trap into page fault exception handler, where it choose different policy according to the state of running kprobe. Because afte 2) the state is KPROBE_HIT_SS, so kernel reset the current kp ---truncated---	5.5	Mo De
CVE-2021-46956	In the Linux kernel, the following vulnerability has been resolved: virtiofs: fix memory leak in virtio_fs_probe() When accidentally passing twice the same tag to qemu, kmemleak ended up reporting a memory leak in virtiofs. Also, looking at the log I saw the following error (that's when I realised the duplicated tag): virtiofs: probe of virtio5 failed with error -17 Here's the kmemleak log for reference: unreferenced object 0xffff888103d47800 (size 1024): comm "systemd-udevd", pid 118, jiffies 4294893780 (age 18.340s) hex dump (first 32 bytes): 00 00 00 00 ad 4e ad de ff ff ff ff 00 00 00 00 .....N..... ff ff ff ff ff ff ff ff 80 90 02 a0 ff ff ff ff ..... backtrace: [<000000000ebb87c1>] virtio_fs_probe+0x171/0x7ae [virtiofs] [<00000000f8aca419>] virtio_dev_probe+0x15f/0x210 [<000000004d6baf3c>] really_probe+0xea/0x430 [<00000000a6ceeac8>] device_driver_attach+0xa8/0xb0 [<00000000196f47a7>] __driver_attach+0x98/0x140 [<000000000b20601d>] bus_for_each_dev+0x7b/0xc0 [<00000000399c7b7f>] bus_add_driver+0x11b/0x1f0 [<0000000032b09ba7>] driver_register+0x8f/0xe0 [<00000000cdd55998>] 0xffffffffa002c013 [<000000000ea196a2>] do_one_initcall+0x64/0x2e0 [<0000000008f727ce>] do_init_module+0x5c/0x260 [<000000003cdedab6>] __do_sys_finit_module+0xb5/0x120 [<00000000ad2f48c6>] do_syscall_64+0x33/0x40 [<00000000809526b5>] entry_SYSCALL_64_after_hwframe+0x44/0xae	5.5	Mo De
CVE-2021-46951	In the Linux kernel, the following vulnerability has been resolved: tpm: efi: Use local variable for calculating final log size When tpm_read_log_efi is called multiple times, which happens when one loads and unloads a TPM2 driver multiple times, then the global variable efi_tpm_final_log_size will at some point become a negative number due to the subtraction of final_events_preboot_size occurring each time. Use a local variable to avoid this integer underflow. The following issue is now resolved: Mar 8 15:35:12 hibinst kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 Mar 8 15:35:12 hibinst kernel: Workqueue: tpm-vtpm vtpm_proxy_work [tpm_vtpm_proxy] Mar 8 15:35:12 hibinst kernel: RIP: 0010:__memcpy+0x12/0x20 Mar 8 15:35:12 hibinst kernel: Code: 00 b8 01 00 00 00 85 d2 74 0a c7 05 44 7b ef 00 0f 00 00 00 c3 cc cc cc 66 66 90 66 90 48 89 f8 48 89 d1 48 c1 e9 03 83 e2 07 <f3> 48 a5 89 d1 f3 a4 c3 66 0f 1f 44 00 00 48 89 f8 48 89 d1 f3 a4 Mar 8 15:35:12 hibinst kernel: RSP: 0018:ffff9ac4c0fcfde0 EFLAGS: 00010206 Mar 8 15:35:12 hibinst kernel: RAX: ffff88f878cefed5 RBX: ffff88f878ce9000 RCX: 1fffffffffffe0f Mar 8 15:35:12 hibinst kernel: RDX: 0000000000000003 RSI: ffff9ac4c003bff9 RDI: ffff88f878cf0e4d Mar 8 15:35:12 hibinst kernel: RBP: ffff9ac4c003b000 R08: 0000000000001000 R09: 000000007e9d6073 Mar 8 15:35:12 hibinst kernel: R10: ffff9ac4c003b000 R11: ffff88f879ad3500 R12: 0000000000000ed5 Mar 8 15:35:12 hibinst kernel: R13: ffff88f878ce9760 R14: 0000000000000002 R15: ffff88f77de7f018 Mar 8 15:35:12 hibinst kernel: FS: 0000000000000000(0000) GS:ffff88f87bd00000(0000) knlGS:0000000000000000 Mar 8 15:35:12 hibinst kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 Mar 8 15:35:12 hibinst kernel: CR2: ffff9ac4c003c000 CR3: 00000001785a6004 CR4: 0000000000060ee0 Mar 8 15:35:12 hibinst kernel: Call Trace: Mar 8 15:35:12 hibinst kernel: tpm_read_log_efi+0x152/0x1a7 Mar 8 15:35:12 hibinst kernel: tpm_bios_log_setup+0xc8/0x1c0 Mar 8 15:35:12 hibinst kernel: tpm_chip_register+0x8f/0x260 Mar 8 15:35:12 hibinst kernel: vtpm_proxy_work+0x16/0x60 [tpm_vtpm_proxy] Mar 8 15:35:12 hibinst kernel: process_one_work+0x1b4/0x370 Mar 8 15:35:12 hibinst kernel: worker_thread+0x53/0x3e0 Mar 8 15:35:12 hibinst kernel: ? process_one_work+0x370/0x370	5.5	Mo De
CVE-2021-46949	In the Linux kernel, the following vulnerability has been resolved: sfc: farch: fix TX queue lookup in TX flush done handling We're starting from a TXQ instance number ('qid'), not a TXQ type, so efx_get_tx_queue() is inappropriate (and could return NULL, leading to panics).	5.5	Mo De
CVE-2021-46948	In the Linux kernel, the following vulnerability has been resolved: sfc: farch: fix TX queue lookup in TX event handling We're starting from a TXQ label, not a TXQ type, so efx_channel_get_tx_queue() is inappropriate (and could return NULL, leading to panics).	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46947	In the Linux kernel, the following vulnerability has been resolved: sfc: adjust efx->xdp_tx_queue_count with the real number of initialized queues efx->xdp_tx_queue_count is initially initialized to num_possible_cpus() and is later used to allocate and traverse efx->xdp_tx_queues lookup array. However, we may end up not initializing all the array slots with real queues during probing. This results, for example, in a NULL pointer dereference, when running "# ethtool -S <iface>", similar to below [2570283.664955][T4126959] BUG: kernel NULL pointer dereference, address: 0000000000000f8 [2570283.681283][T4126959] #PF: supervisor read access in kernel mode [2570283.695678][T4126959] #PF: error_code(0x0000) - not-present page [2570283.710013][T4126959] PGD 0 P4D 0 [2570283.721649][T4126959] Oops: 0000 [#1] SMP PTI [2570283.734108][T4126959] CPU: 23 PID: 4126959 Comm: ethtool Tainted: G O 5.10.20-cloudflare-2021.3.1 #1 [2570283.752641][T4126959] Hardware name: <redacted> [2570283.781408][T4126959] RIP: 0010:efx_ethtool_get_stats+0x2ca/0x330 [sfc] [2570283.796073][T4126959] Code: 00 85 c0 74 39 48 8b 95 a8 0f 00 00 48 85 d2 74 2d 31 c0 eb 07 48 8b 95 a8 0f 00 00 48 63 c8 49 83 c4 08 83 c0 01 48 8b 14 ca <48> 8b 92 f8 00 00 00 49 89 54 24 f8 39 85 a0 0f 00 00 77 d7 48 8b [2570283.831259][T4126959] RSP: 0018:ffffb79a77657ce8 EFLAGS: 00010202 [2570283.845121][T4126959] RAX: 0000000000000019 RBX: ffffb799cd0c9280 RCX: 0000000000000018 [2570283.860872][T4126959] RDX: 0000000000000000 RSI: ffff96dd970ce000 RDI: 0000000000000005 [2570283.876525][T4126959] RBP: ffff96dd86f0a000 R08: ffff96dd970ce480 R09: 000000000000005f [2570283.892014][T4126959] R10: ffffb799cd0c9fff R11: ffffb799cd0c9000 R12: ffffb799cd0c94f8 [2570283.907406][T4126959] R13: ffffffffc11b1090 R14: ffff96dd970ce000 R15: ffffffffc11cd66c [2570283.922705][T4126959] FS: 00007fa7723f8740(0000) GS:ffff96f51fac0000(0000) knlGS:0000000000000000 [2570283.938848][T4126959] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [2570283.952524][T4126959] CR2: 00000000000000f8 CR3: 0000001a73e6e006 CR4: 00000000007706e0 [2570283.967529][T4126959] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [2570283.982400][T4126959] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [2570283.997308][T4126959] PKRU: 55555554 [2570284.007649][T4126959] Call Trace: [2570284.017598][T4126959] dev_ethtool+0x1832/0x2830 Fix this by adjusting efx->xdp_tx_queue_count after probing to reflect the true value of initialized slots in efx->xdp_tx_queues.	5.5	Mo De
CVE-2021-46944	In the Linux kernel, the following vulnerability has been resolved: media: staging/intel-ipu3: Fix memory leak in imu_fmt We are losing the reference to an allocated memory if try. Change the order of the check to avoid that.	5.5	Mo De
CVE-2023-52448	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix kernel NULL pointer dereference in gfs2_rgrp_dump Syzkaller has reported a NULL pointer dereference when accessing rgd->rd_rgl in gfs2_rgrp_dump(). This can happen when creating rgd->rd_gl fails in read_rindex_entry(). Add a NULL pointer check in gfs2_rgrp_dump() to prevent that.	5.5	Mo De
CVE-2024-1704	A vulnerability was found in ZhongBangKeJi CRMEB 5.2.2. It has been declared as critical. This vulnerability affects the function save/delete of the file /adminapi/system/crud. The manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254392. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	Mo De
CVE-2023-52449	In the Linux kernel, the following vulnerability has been resolved: mtd: Fix gluebi NULL pointer dereference caused by ftl notifier If both ftl.ko and gluebi.ko are loaded, the notifier of ftl triggers NULL pointer dereference when trying to access 'gluebi->desc' in gluebi_read(). ubi_gluebi_init ubi_register_volume_notifier ubi_enumerate_volumes ubi_notify_all gluebi_notify nb->notifier_call() gluebi_create mtd_device_register mtd_device_parse_register add_mtd_device blktrans_notify_add not->add() ftl_add_mtd tr->add_mtd() scan_header mtd_read mtd_read_oob mtd_read_oob_std gluebi_read mtd->read() gluebi->desc - NULL Detailed reproduction information available at the Link [1], In the normal case, obtain gluebi->desc in the gluebi_get_device(), and access gluebi->desc in the gluebi_read(). However, gluebi_get_device() is not executed in advance in the ftl_add_mtd() process, which leads to NULL pointer dereference. The solution for the gluebi module is to run jffs2 on the UBI volume without considering working with ftl or mtdblock [2]. Therefore, this problem can be avoided by preventing gluebi from creating the mtdblock device after creating mtd partition of the type MTD_UBIVOLUME.	5.5	Mo De
CVE-2023-52450	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel/uncore: Fix NULL pointer dereference issue in upi_fill_topology() Get logical socket id instead of physical id in discover_upi_topology() to avoid out-of-bound access on 'upi = &type->topology[nid][idx];' line that leads to NULL pointer dereference in upi_fill_topology()	5.5	Mo De
CVE-2024-26587	In the Linux kernel, the following vulnerability has been resolved: net: netdevsim: don't try to destroy PHC on VFs PHC gets initialized in nsim_init_netdevsim(), which is only called if (nsim_dev_port_is_pf()). Create a counterpart of nsim_init_netdevsim() and move the mock_phc_destroy() there. This fixes a crash trying to destroy netdevsim with VFs instantiated, as caught by running the devlink.sh test: BUG: kernel NULL pointer dereference, address: 00000000000000b8 RIP: 0010:mock_phc_destroy+0xd/0x30 Call Trace: <TASK> nsim_destroy+0x4a/0x70 [netdevsim] __nsim_dev_port_del+0x47/0x70 [netdevsim] nsim_dev_reload_destroy+0x105/0x120 [netdevsim] nsim_drv_remove+0x2f/0xb0 [netdevsim] device_release_driver_internal+0x1a1/0x210 bus_remove_device+0xd5/0x120 device_del+0x159/0x490 device_unregister+0x12/0x30 del_device_store+0x11a/0x1a0 [netdevsim] kernfs_fop_write_iter+0x130/0x1d0 vfs_write+0x30b/0x4b0 ksys_write+0x69/0xf0 do_syscall_64+0xcc/0x1e0 entry_SYSCALL_64_after_hwframe+0x6f/0x77	5.5	Mo De
CVE-2024-26590	In the Linux kernel, the following vulnerability has been resolved: erofs: fix inconsistent per-file compression format EROFS can select compression algorithms on a per-file basis, and each per-file compression algorithm needs to be marked in the on-disk superblock for initialization. However, syzkaller can generate inconsistent crafted images that use an unsupported algorithmtype for specific inodes, e.g. use MicroLZMA algorithmtype even it's not set in `sbi->available_compr_algs`. This can lead to an unexpected "BUG: kernel NULL pointer dereference" if the corresponding decompressor isn't built-in. Fix this by checking against `sbi->available_compr_algs` for each m_algorithmformat request. Incorrect !erofs_sb_has_compr_cfgs preset bitmap is now fixed together since it was harmless previously.	5.5	Mo De
CVE-2024-26591	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix re-attachment branch in bpf_tracing_prog_attach The following case can cause a crash due to missing attach_btf: 1) load rawtp program 2) load fentry program with rawtp as target_fd 3) create tracing link for fentry program with target_fd = 0 4) repeat 3 In the end we have: - prog->aux->dst_trampoline == NULL - tgt_prog == NULL (because we did not provide target_fd to link_create) - prog->aux->attach_btf == NULL (the program was loaded with attach_prog_fd=X) - the program was loaded for tgt_prog but we have no way to find out which one BUG: kernel NULL pointer dereference, address: 0000000000000058 Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x15b/0x430 ? fixup_exception+0x22/0x330 ? exc_page_fault+0x6f/0x170 ? asm_exc_page_fault+0x22/0x30 ? bpf_tracing_prog_attach+0x279/0x560 ? btf_obj_id+0x5/0x10 bpf_tracing_prog_attach+0x439/0x560 __sys_bpf+0x1cf4/0x2de0 __x64_sys_bpf+0x1c/0x30 do_syscall_64+0x41/0xf0 entry_SYSCALL_64_after_hwframe+0x6e/0x76 Return -EINVAL in this situation.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46942	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix shared sqpoll cancellation hangs [736.982891] INFO: task iou-sqp-4294:4295 blocked for more than 122 seconds. [736.982897] Call Trace: [736.982901] schedule+0x68/0xe0 [736.982903] io_uring_cancel_sqpoll+0xdb/0x110 [736.982908] io_sqpoll_cancel_cb+0x24/0x30 [736.982911] io_run_task_work_head+0x28/0x50 [736.982913] io_sq_thread+0x4e3/0x720 We call io_uring_cancel_sqpoll() one by one for each ctx either in sq_thread() itself or via task works, and it's intended to cancel all requests of a specified context. However the function uses per-task counters to track the number of inflight requests, so it counts more requests than available via currect io_uring ctx and goes to sleep for them to appear (e.g. from IRQ), that will never happen. Cancel a bit more than before, i.e. all ctxs that share sqpoll and continue to use shared counters. Don't forget that we should not remove ctx from the list before running that task_work sqpoll-cancel, otherwise the function wouldn't be able to find the context and will hang.	5.5	Mo De
CVE-2021-46941	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: core: Do core softreset when switch mode According to the programming guide, to switch mode for DRD controller, the driver needs to do the following. To switch from device to host: 1. Reset controller with GCTL.CoreSoftReset 2. Set GCTL.PrtCapDir(host mode) 3. Reset the host with USBCMD.HCRESET 4. Then follow up with the initializing host registers sequence To switch from host to device: 1. Reset controller with GCTL.CoreSoftReset 2. Set GCTL.PrtCapDir(device mode) 3. Reset the device with DCTL.CSftRst 4. Then follow up with the initializing registers sequence Currently we're missing step 1) to do GCTL.CoreSoftReset and step 3) of switching from host to device. John Stult reported a lockup issue seen with HiKey960 platform without these steps[1]. Similar issue is observed with Ferry's testing platform[2]. So, apply the required steps along with some fixes to Yu Chen's and John Stultz's version. The main fixes to their versions are the missing wait for clocks synchronization before clearing GCTL.CoreSoftReset and only apply DCTL.CSftRst when switching from host to device. [1] https://lore.kernel.org/linux-usb/20210108015115.27920-1-john.stultz@linaro.org/ [2] https://lore.kernel.org/linux-usb/0ba7a6ba-e6a7-9cd4-0695-64fc927e01f1@gmail.com/	5.5	Mo De
CVE-2021-46940	In the Linux kernel, the following vulnerability has been resolved: tools/power turbostat: Fix offset overflow issue in index converting The idx_to_offset() function returns type int (32-bit signed), but MSR_PKG_ENERGY_STAT is u32 and would be interpreted as a negative number. The end result is that it hits the if (offset < 0) check in update_msr_sum() which prevents the timer callback from updating the stat in the background when long durations are used. The similar issue exists in offset_to_idx() and update_msr_sum(). Fix this issue by converting the 'int' to 'off_t' accordingly.	5.5	Mo De
CVE-2021-46961	In the Linux kernel, the following vulnerability has been resolved: irqchip/gic-v3: Do not enable irqs when handling spurious interrups We triggered the following error while running our 4.19 kernel with the pseudo-NMI patches backported to it: [14.816231] ------------[cut here]------------ [14.816231] kernel BUG at irq.c:99! [14.816232] Internal error: Oops - BUG: 0 [#1] SMP [14.816232] Process swapper/0 (pid: 0, stack limit = 0x(____ptrval____)) [14.816233] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G O 4.19.95.aarch64 #14 [14.816233] Hardware name: evb (DT) [14.816234] pstate: 80400085 (Nzcv daIf +PAN -UAO) [14.816234] pc : asm_nmi_enter+0x94/0x98 [14.816235] lr : asm_nmi_enter+0x18/0x98 [14.816235] sp : ffff000008003c50 [14.816235] pmr_save: 00000070 [14.816237] x29: ffff000008003c50 x28: ffff0000095f56c0 [14.816238] x27: 0000000000000000 x26: ffff000008004000 [14.816239] x25: 00000000015e0000 x24: ffff8008fb916000 [14.816240] x23: 0000000020400005 x22: ffff0000080817cc [14.816241] x21: ffff000008003da0 x20: 0000000000000060 [14.816242] x19: 00000000000003ff x18: ffffffffffffffff [14.816243] x17: 0000000000000008 x16: 003d090000000000 [14.816244] x15: ffff0000095ea6c8 x14: ffff8008fff5ab40 [14.816244] x13: ffff8008fff58b9d x12: 0000000000000000 [14.816245] x11: ffff000008c8a200 x10: 000000008e31fca5 [14.816246] x9 : ffff000008c8a208 x8 : 000000000000000f [14.816247] x7 : 0000000000000004 x6 : ffff8008fff58b9e [14.816248] x5 : 0000000000000000 x4 : 0000000080000000 [14.816249] x3 : 0000000000000000 x2 : 0000000080000000 [14.816250] x1 : 0000000000120000 x0 : ffff0000095f56c0 [14.816251] Call trace: [14.816251] asm_nmi_enter+0x94/0x98 [14.816251] el1_irq+0x8c/0x180 (IRQ C) [14.816252] gic_handle_irq+0xbc/0x2e4 [14.816252] el1_irq+0xcc/0x180 (IRQ B) [14.816253] arch_timer_handler_virt+0x38/0x58 [14.816253] handle_percpu_devid_irq+0x90/0x240 [14.816253] generic_handle_irq+0x34/0x50 [14.816254] __handle_domain_irq+0x68/0xc0 [14.816254] gic_handle_irq+0xf8/0x2e4 [14.816255] el1_irq+0xcc/0x180 (IRQ A) [14.816255] arch_cpu_idle+0x34/0x1c8 [14.816255] default_idle_call+0x24/0x44 [14.816256] do_idle+0x1d0/0x2c8 [14.816256] cpu_startup_entry+0x28/0x30 [14.816256] rest_init+0xb8/0xc8 [14.816257] start_kernel+0x4c8/0x4f4 [14.816257] Code: 940587f1 d5384100 b9401001 36a7fd01 (d4210000) [14.816258] Modules linked in: start_dp(O) smeth(O) [15.103092] ---[end trace 701753956cb14aa8]--- [15.103093] Kernel panic - not syncing: Fatal exception in interrupt [15.103099] SMP: stopping secondary CPUs [15.103100] Kernel Offset: disabled [15.103100] CPU features: 0x36,a2400218 [15.103100] Memory Limit: none which is cause by a 'BUG_ON(in_nmi())' in nmi_enter(). From the call trace, we can find three interrupts (noted A, B, C above): interrupt (A) is preempted by (B), which is further interrupted by (C). Subsequent investigations show that (B) results in nmi_enter() being called, but that it actually is a spurious interrupt. Furthermore, interrupts are reenabled in the context of (B), and (C) fires with NMI priority. We end-up with a nested NMI situation, something we definitely do not want to (and cannot) handle. The bug here is that spurious interrupts should never result in any state change, and we should just return to the interrupted context. Moving the handling of spurious interrupts as early as possible in the GICv3 handler fixes this issue. [maz: rewrote commit message, corrected Fixes: tag]	5.5	Mo De
CVE-2024-26133	EventStoreDB (ESDB) is an operational database built to store events. A vulnerability has been identified in the projections subsystem in versions 20 prior to 20.10.6, 21 prior to 21.10.11, 22 prior to 22.10.5, and 23 prior to 23.10.1. Only database instances that use custom projections are affected by this vulnerability. User passwords may become accessible to those who have access to the chunk files on disk, and users who have read access to system streams. Only users in the `$admins` group can access system streams by default. ESDB 23.10.1, 22.10.5, 21.10.11, and 20.10.6 contain a patch for this issue. Users should upgrade EventStoreDB, reset the passwords for current and previous members of `$admins` and `$ops` groups, and, if a password was reused in any other system, reset it in those systems to a unique password to follow best practices. If an upgrade cannot be done immediately, reset the passwords for current and previous members of `$admins` and `$ops` groups. Avoid creating custom projections until the patch has been applied.	5.5	Mo De
CVE-2020-36776	In the Linux kernel, the following vulnerability has been resolved: thermal/drivers/cpufreq_cooling: Fix slab OOB issue Slab OOB issue is scanned by KASAN in cpu_power_to_freq(). If power is limited below the power of OPP0 in EM table, it will cause slab out-of-bound issue with negative array index. Return the lowest frequency if limited power cannot found a suitable OPP in EM table to fix this issue. Backtrace: [<ffffffd02d2a37f0>] die+0x104/0x5ac [<ffffffd02d2a5630>] bug_handler+0x64/0xd0 [<ffffffd02d288ce4>] brk_handler+0x160/0x258 [<ffffffd02d281e5c>] do_debug_exception+0x248/0x3f0 [<ffffffd02d284488>] el1_dbg+0x14/0xbc [<ffffffd02d75d1d4>] __kasan_report+0x1dc/0x1e0 [<ffffffd02d75c2e0>] kasan_report+0x10/0x20 [<ffffffd02d75def8>] __asan_report_load8_noabort+0x18/0x28 [<ffffffd02e6fce5c>] cpufreq_power2state+0x180/0x43c [<ffffffd02e6ead80>] power_actor_set_power+0x114/0x1d4 [<ffffffd02e6fac24>] allocate_power+0xaec/0xde0 [<ffffffd02e6f9f80>] power_allocator_throttle+0x3ec/0x5a4 [<ffffffd02e6ea888>] handle_thermal_trip+0x160/0x294 [<ffffffd02e6edd08>] thermal_zone_device_check+0xe4/0x154 [<ffffffd02d351cb4>] process_one_work+0x5e4/0xe28 [<ffffffd02d352f44>] worker_thread+0xa4c/0xfac [<ffffffd02d360124>] kthread+0x33c/0x358 [<ffffffd02d289940>] ret_from_fork+0xc/0x18	5.5	Mo De
CVE-2023-42877	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to modify protected parts of the file system.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2023-42823	The issue was resolved by sanitizing logging This issue is fixed in watchOS 10.1, macOS Sonoma 14.1, tvOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, macOS Ventura 13.6.1. An app may be able to access user-sensitive data.	5.5	Mc De
CVE-2023-42834	A privacy issue was addressed with improved handling of files. This issue is fixed in watchOS 10.1, macOS Sonoma 14.1, macOS Monterey 12.7.2, macOS Ventura 13.6.3, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	5.5	Mc De
CVE-2023-42839	This issue was addressed with improved state management. This issue is fixed in tvOS 17.1, watchOS 10.1, macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	5.5	Mc De
CVE-2023-42840	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access user-sensitive data.	5.5	Mc De
CVE-2023-42853	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access user-sensitive data.	5.5	Mc De
CVE-2023-42858	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access user-sensitive data.	5.5	Mc De
CVE-2023-42859	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to modify protected parts of the file system.	5.5	Mc De
CVE-2023-42860	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to modify protected parts of the file system.	5.5	Mc De
CVE-2023-42878	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in watchOS 10.1, macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	5.5	Mc De
CVE-2021-46962	In the Linux kernel, the following vulnerability has been resolved: mmc: uniphier-sd: Fix a resource leak in the remove function A 'tmio_mmc_host_free()' call is missing in the remove function, in order to balance a 'tmio_mmc_host_alloc()' call in the probe. This is done in the error handling path of the probe, but not in the remove function. Add the missing call.	5.5	Mc De
CVE-2023-42889	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to bypass certain Privacy preferences.	5.5	Mc De
CVE-2023-42945	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1. An app may gain unauthorized access to Bluetooth.	5.5	Mc De
CVE-2023-42946	This issue was addressed with improved redaction of sensitive information. This issue is fixed in tvOS 17.1, watchOS 10.1, macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to leak sensitive user information.	5.5	Mc De
CVE-2023-42953	A permissions issue was addressed with additional restrictions. This issue is fixed in tvOS 17.1, watchOS 10.1, macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	5.5	Mc De
CVE-2023-52442	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate session id and tree id in compound request `smb2_get_msg()` in smb2_get_ksmbd_tcon() and smb2_check_user_session() will always return the first request smb2 header in a compound request. if `SMB2_TREE_CONNECT_HE` is the first command in compound request, will return 0, i.e. The tree id check is skipped. This patch use ksmbd_req_buf_next() to get current command in compound.	5.5	Mc De
CVE-2021-46967	In the Linux kernel, the following vulnerability has been resolved: vhost-vdpa: fix vm_flags for virtqueue doorbell mapping The virtqueue doorbell is usually implemented via registeres but we don't provide the necessary vma->flags like VM_PFNMAP. This may cause several issues e.g when userspace tries to map the doorbell via vhost IOTLB, kernel may panic due to the page is not backed by page structure. This patch fixes this by setting the necessary vm_flags. With this patch, try to map doorbell via IOTLB will fail with bad address.	5.5	Mc De
CVE-2024-26584	In the Linux kernel, the following vulnerability has been resolved: net: tls: handle backlogging of crypto requests Since we're setting the CRYPTO_TFM_REQ_MAY_BACKLOG flag on our requests to the crypto API, crypto_aead_{encrypt,decrypt} can return -EBUSY instead of -EINPROGRESS in valid situations. For example, when the cryptd queue for AESNI is full (easy to trigger with an artificially low cryptd.cryptd_max_cpu_qlen), requests will be enqueued to the backlog but still processed. In that case, the async callback will also be called twice: first with err == -EINPROGRESS, which it seems we can just ignore, then with err == 0. Compared to Sabrina's original patch this version uses the new tls_*crypt_async_wait() helpers and converts the EBUSY to EINPROGRESS to avoid having to modify all the error handling paths. The handling is identical.	5.5	Mc De

CVE Number	Description	Base Score	Re
CVE-2021-46963	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix crash in qla2xxx_mqueuecommand() RIP: 0010:kmem_cache_free+0xfa/0x1b0 Call Trace: qla2xxx_mqueuecommand+0x2b5/0x2c0 [qla2xxx] scsi_queue_rq+0x5e2/0xa40 __blk_mq_try_issue_directly+0x128/0x1d0 blk_mq_request_issue_directly+0x4e/0xb0 Fix incorrect call to free srb in qla2xxx_mqueuecommand(), as srb is now allocated by upper layers. This fixes smatch warning of srb unintended free.	5.5	Mo De
CVE-2021-46939	In the Linux kernel, the following vulnerability has been resolved: tracing: Restructure trace_clock_global() to never block It was reported that a fix to the ring buffer recursion detection would cause a hung machine when performing suspend / resume testing. The following backtrace was extracted from debugging that case: Call Trace: trace_clock_global+0x91/0xa0 __rb_reserve_next+0x237/0x460 ring_buffer_lock_reserve+0x12a/0x3f0 trace_buffer_lock_reserve+0x10/0x50 __trace_graph_return+0x1f/0x80 trace_graph_return+0xb7/0xf0 ? trace_clock_global+0x91/0xa0 ftrace_return_to_handler+0x8b/0xf0 ? pv_hash+0xa0/0xa0 return_to_handler+0x15/0x30 ? ftrace_graph_caller+0xa0/0xa0 ? trace_clock_global+0x91/0xa0 ? __rb_reserve_next+0x237/0x460 ? ring_buffer_lock_reserve+0x12a/0x3f0 ? trace_event_buffer_lock_reserve+0x3c/0x120 ? trace_event_buffer_reserve+0x6b/0xc0 ? trace_event_raw_event_device_pm_callback_start+0x125/0x2d0 ? dpm_run_callback+0x3b/0xc0 ? pm_ops_is_empty+0x50/0x50 ? platform_get_irq_byname_optional+0x90/0x90 ? trace_device_pm_callback_start+0x82/0xd0 ? dpm_run_callback+0x49/0xc0 With the following RIP: RIP: 0010:native_queued_spin_lock_slowpath+0x69/0x200 Since the fix to the recursion detection would allow a single recursion to happen while tracing, this lead to the trace_clock_global() taking a spin lock and then trying to take it again: ring_buffer_lock_reserve() { trace_clock_global() { arch_spin_lock() { queued_spin_lock_slowpath() { /* lock taken */ (something else gets traced by function graph tracer) ring_buffer_lock_reserve() { trace_clock_global() { arch_spin_lock() { queued_spin_lock_slowpath() { /* DEAD LOCK! */ Tracing should *never* block, as it can lead to strange lockups like the above. Restructure the trace_clock_global() code to instead of simply taking a lock to update the recorded "prev_time" simply use it, as two events happening on two different CPUs that calls this at the same time, really doesn't matter which one goes first. Use a trylock to grab the lock for updating the prev_time, and if it fails, simply try again the next time. If it failed to be taken, that means something else is already updating it. Bugzilla: https://bugzilla.kernel.org/show_bug.cgi?id=212761	5.5	Mo De
CVE-2021-46945	In the Linux kernel, the following vulnerability has been resolved: ext4: always panic when errors=panic is specified Before commit 014c9caa29d3 ("ext4: make ext4_abort() use __ext4_error()"), the following series of commands would trigger a panic: 1. mount /dev/sda -o ro,errors=panic test 2. mount /dev/sda -o remount,abort test After commit 014c9caa29d3, remounting a file system using the test mount option "abort" will no longer trigger a panic. This commit will restore the behaviour immediately before commit 014c9caa29d3. (However, note that the Linux kernel's behavior has not been consistent; some previous kernel versions, including 5.4 and 4.19 similarly did not panic after using the mount option "abort".) This also makes a change to long-standing behaviour; namely, the following series commands will now cause a panic, when previously it did not: 1. mount /dev/sda -o ro,errors=panic test 2. echo test > /sys/fs/ext4/sda/trigger_fs_error However, this makes ext4's behaviour much more consistent, so this is a good thing.	5.5	Mo De
CVE-2023-52463	In the Linux kernel, the following vulnerability has been resolved: efivarfs: force RO when remounting if SetVariable is not supported If SetVariable at runtime is not supported by the firmware we never assign a callback for that function. At the same time mount the efivarfs as RO so no one can call that. However, we never check the permission flags when someone remounts the filesystem as RW. As a result this leads to a crash looking like this: $ mount -o remount,rw /sys/firmware/efi/efivars $ efi-updatevar -f PK.auth PK [303.279166] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [303.280482] Mem abort info: [303.280854] ESR = 0x0000000086000004 [303.281338] EC = 0x21: IABT (current EL), IL = 32 bits [303.282016] SET = 0, FnV = 0 [303.282414] EA = 0, S1PTW = 0 [303.282821] FSC = 0x04: level 0 translation fault [303.283771] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000042 58c000 [303.284913] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 [303.286076] Internal error: Oops: 0000000086000004 [#1] PREEMPT SMP [303.286936] Modules linked in: qrtr tpm_tis tpm_tis_core crct10dif_ce arm_smccc_trng rng_core drm fuse ip_tables x_tables ipv6 [303.288586] CPU: 1 PID: 755 Comm: efi-updatevar Not tainted 6.3.0-rc1-00108-gc7d0c4695c68 #1 [303.289748] Hardware name: Unknown Unknown Product/Unknown Product, BIOS 2023.04-00627-g88336918701d 04/01/2023 [303.291150] pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [303.292123] pc : 0x0 [303.292443] lr : efivar_set_variable_locked+0x74/0xec [303.293156] sp : ffff800008673c10 [303.293619] x29: ffff800008673c10 x28: ffff0000037e8000 x27: 0000000000000000 [303.294592] x26: 0000000000000800 x25: ffff000002467400 x24: 0000000000000027 [303.295572] x23: ffffd49ea9832000 x22: ffff0000020c9800 x21: ffff000002467000 [303.296566] x20: 0000000000000001 x19: 00000000000007fc x18: 0000000000000000 [303.297531] x17: 0000000000000000 x16: 0000000000000000 x15: 0000aaaac807ab54 [303.298495] x14: ed37489f673633c0 x13: 71c45c606de13f80 x12: 47464259e219acf4 [303.299453] x11: ffff000002af7b01 x10: 0000000000000003 x9 : 0000000000000002 [303.300431] x8 : 0000000000000010 x7 : ffffd49ea8973230 x6 : 0000000000a85201 [303.301412] x5 : 0000000000000000 x4 : ffff0000020c9800 x3 : 00000000000007fc [303.302370] x2 : 0000000000000027 x1 : ffff000002467400 x0 : ffff000002467000 [303.303341] Call trace: [303.303679] 0x0 [303.303938] efivar_entry_set_get_size+0x98/0x16c [303.304585] efivarfs_file_write+0xd0/0x1a4 [303.305148] vfs_write+0xc4/0x2e4 [303.305601] ksys_write+0x70/0x104 [303.306073] __arm64_sys_write+0x1c/0x28 [303.306622] invoke_syscall+0x48/0x114 [303.307156] el0_svc_common.constprop.0+0x44/0xec [303.307803] do_el0_svc+0x38/0x98 [303.308268] el0_svc+0x2c/0x84 [303.308702] el0t_64_sync_handler+0xf4/0x120 [303.309293] el0t_64_sync+0x190/0x194 [303.309794] Code: ???????? ???????? ???????? ???????? (????????) [303.310612] ---[end trace 0000000000000000]--- Fix this by adding a .reconfigure() function to the fs operations which we can use to check the requested flags and deny anything that's not RO if the firmware doesn't implement SetVariable at runtime.	5.5	Mo De
CVE-2023-52453	In the Linux kernel, the following vulnerability has been resolved: hisi_acc_vfio_pci: Update migration data pointer correctly on saving/resume When the optional PRE_COPY support was added to speed up the device compatibility check, it failed to update the saving/resuming data pointers based on the fd offset. This results in migration data corruption and when the device gets started on the destination the following error is reported in some cases, [478.907684] arm-smmu-v3 arm-smmu-v3.2.auto: event 0x10 received: [478.913691] arm-smmu-v3 arm-smmu-v3.2.auto: 0x0000310200000010 [478.919603] arm-smmu-v3 arm-smmu-v3.2.auto: 0x000002088000007f [478.925515] arm-smmu-v3 arm-smmu-v3.2.auto: 0x0000000000000000 [478.931425] arm-smmu-v3 arm-smmu-v3.2.auto: 0x0000000000000000 [478.947552] hisi_zip 0000:31:00.0: qm_axi_rresp [error status=0x1] found [478.955930] hisi_zip 0000:31:00.0: qm_db_timeout [error status=0x400] found [478.955944] hisi_zip 0000:31:00.0: qm sq doorbell timeout in function 2	5.5	Mo De
CVE-2023-52462	In the Linux kernel, the following vulnerability has been resolved: bpf: fix check for attempt to corrupt spilled pointer When register is spilled onto a stack as a 1/2/4-byte register, we set slot_type[BPF_REG_SIZE - 1] (plus potentially few more below it, depending on actual spill size). So to check if some stack slot has spilled register we need to consult slot_type[7], not slot_type[0]. To avoid the need to remember and double-check this in the future, just use is_spilled_reg() helper.	5.5	Mo De
CVE-2024-1821	A vulnerability was found in code-projects Crime Reporting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file police_add.php. The manipulation of the argument police_name/police_id/police_spec/password leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-254609 was assigned to this vulnerability.	5.5	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26595	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_acl_tcam: Fix NULL pointer dereference in error path When calling mlxsw_sp_acl_tcam_region_destroy() from an error path after failing to attach the region to an ACL group, we hit a NULL pointer dereference upon 'region->group->tcam' [1]. Fix by retrieving the 'tcam' pointer using mlxsw_sp_acl_to_tcam(). [1] BUG: kernel NULL pointer dereference, address: 0000000000000000 [...] RIP: 0010:mlxsw_sp_acl_tcam_region_destroy+0xa0/0xd0 [...] Call Trace: mlxsw_sp_acl_tcam_vchunk_get+0x88b/0xa20 mlxsw_sp_acl_tcam_ventry_add+0x25/0xe0 mlxsw_sp_acl_rule_add+0x47/0x240 mlxsw_sp_flower_replace+0x1a9/0x1d0 tc_setup_cb_add+0xdc/0x1c0 fl_hw_replace_filter+0x146/0x1f0 fl_change+0xc17/0x1360 tc_new_tfilter+0x472/0xb90 rtnetlink_rcv_msg+0x313/0x3b0 netlink_rcv_skb+0x58/0x100 netlink_unicast+0x244/0x390 netlink_sendmsg+0x1e4/0x440 ____sys_sendmsg+0x164/0x260 ___sys_sendmsg+0x9a/0xe0 __sys_sendmsg+0x7a/0xc0 do_syscall_64+0x40/0xe0 entry_SYSCALL_64_after_hwframe+0x63/0x6b	5.5	Mo De
CVE-2023-52460	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL pointer dereference at hibernate During hibernate sequence the source context might not have a clk_mgr. So don't use it to look for DML2 support.	5.5	Mo De
CVE-2023-52458	In the Linux kernel, the following vulnerability has been resolved: block: add check that partition length needs to be aligned with block size Before calling add partition or resize partition, there is no check on whether the length is aligned with the logical block size. If the logical block size of the disk is larger than 512 bytes, then the partition size maybe not the multiple of the logical block size, and when the last sector is read, bio_truncate() will adjust the bio size, resulting in an IO error if the size of the read command is smaller than the logical block size.If integrity data is supported, this will also result in a null pointer dereference when calling bio_integrity_free.	5.5	Mo De
CVE-2023-52456	In the Linux kernel, the following vulnerability has been resolved: serial: imx: fix tx statemachine deadlock When using the serial port as RS485 port, the tx statemachine is used to control the RTS pin to drive the RS485 transceiver TX_EN pin. When the TTY port is closed in the middle of a transmission (for instance during userland application crash), imx_uart_shutdown disables the interface and disables the Transmission Complete interrupt. afer that, imx_uart_stop_tx bails on an incomplete transmission, to be retriggered by the TC interrupt. This interrupt is disabled and therefore the tx statemachine never transitions out of SEND. The statemachine is in deadlock now, and the TX_EN remains low, making the interface useless. imx_uart_stop_tx now checks for incomplete transmission AND whether TC interrupts are enabled before bailing to be retriggered. This makes sure the state machine handling is reached, and is properly set to WAIT_AFTER_SEND.	5.5	Mo De
CVE-2023-52454	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: Fix a kernel panic when host sends an invalid H2C PDU length If the host sends an H2CData command with an invalid DATAL, the kernel may crash in nvmet_tcp_build_pdu_iovec(). Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 lr : nvmet_tcp_io_work+0x6ac/0x718 [nvmet_tcp] Call trace: process_one_work+0x174/0x3c8 worker_thread+0x2d0/0x3e8 kthread+0x104/0x110 Fix the bug by raising a fatal error if DATAL isn't coherent with the packet size. Also, the PDU length should never exceed the MAXH2CDATA parameter which has been communicated to the host in nvmet_tcp_handle_icreq().	5.5	Mo De
CVE-2023-52459	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Fix duplicated list deletion The list deletion call dropped here is already called from the helper function in the line before. Having a second list_del() call results in either a warning (with CONFIG_DEBUG_LIST=y): list_del corruption, c46c8198->next is LIST_POISON1 (00000100) If CONFIG_DEBUG_LIST is disabled the operation results in a kernel error due to NULL pointer dereference.	5.5	Mo De
CVE-2024-26596	In the Linux kernel, the following vulnerability has been resolved: net: dsa: fix netdev_priv() dereference before check on non-DSA netdevice events After the blamed commit, we started doing this dereference for every NETDEV_CHANGEUPPER and NETDEV_PRECHANGEUPPER event in the system. static inline struct dsa_port *dsa_user_to_port(const struct net_device *dev) { struct dsa_user_priv *p = netdev_priv(dev); return p->dp; } Which is obviously bogus, because not all net_devices have a netdev_priv() of type struct dsa_user_priv. But struct dsa_user_priv is fairly small, and p->dp means dereferencing 8 bytes starting with offset 16. Most drivers allocate that much private memory anyway, making our access not fault, and we discard the bogus data quickly afterwards, so this wasn't caught. But the dummy interface is somewhat special in that it calls alloc_netdev() with a priv size of 0. So every netdev_priv() dereference is invalid, and we get this when we emit a NETDEV_PRECHANGEUPPER event with a VLAN as its new upper: $ ip link add dummy1 type dummy $ ip link add link dummy1 name dummy1.100 type vlan id 100 [43.309174] == [43.316456] BUG: KASAN: slab-out-of-bounds in dsa_user_prechangeupper+0x30/0xe8 [43.323835] Read of size 8 at addr ffff3f86481d2990 by task ip/374 [43.330058] [43.342436] Call trace: [43.366542] dsa_user_prechangeupper+0x30/0xe8 [43.371024] dsa_user_netdevice_event+0xb38/0xee8 [43.375768] notifier_call_chain+0xa4/0x210 [43.379985] raw_notifier_call_chain+0x24/0x38 [43.384464] __netdev_upper_dev_link+0x3ec/0x5d8 [43.389120] netdev_upper_dev_link+0x70/0xa8 [43.393424] register_vlan_dev+0x1bc/0x310 [43.397554] vlan_newlink+0x210/0x248 [43.401247] rtnl_newlink+0x9fc/0xe30 [43.404942] rtnetlink_rcv_msg+0x378/0x580 Avoid the kernel oops by dereferencing after the type check, as customary.	5.5	Mo De
CVE-2024-25130	Tuleap is an open source suite to improve management of software developments and collaboration. Prior to version 15.5.99.76 of Tuleap Community Edition and prior to versions 15.5-4 and 15.4-7 of Tuleap Enterprise Edition, users with a read access to a tracker where the mass update feature is used might get access to restricted information. Tuleap Community Edition 15.5.99.76, Tuleap Enterprise Edition 15.5-4, and Tuleap Enterprise Edition 15.4-7 contain a patch for this issue.	5.4	Mo De
CVE-2024-25151	The Calendar module in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions does not escape user supplied data in the default notification email template, which allows remote authenticated users to inject arbitrary web script or HTML via the title of a calendar event or the user's name. This may lead to a content spoofing or cross-site scripting (XSS) attacks depending on the capability of the receiver's mail client.	5.4	Mo De
CVE-2024-26490	A cross-site scripting (XSS) vulnerability in the Addon JD Simple module of flusity-CMS v2.33 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title text field.	5.4	Mo De
CVE-2024-23349	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Answer.This issue affects Apache Answer: through 1.2.1. XSS attack when user enters summary. A logged-in user, when modifying their own submitted question, can input malicious code in the summary to create such an attack. Users are recommended to upgrade to version [1.2.5], which fixes the issue.	5.4	Mo De
CVE-2023-33843	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256544.	5.4	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-25873	Enhavo v0.13.1 was discovered to contain an HTML injection vulnerability in the Author text field under the Blockquote module. This vulnerability allows attackers to execute arbitrary code via a crafted payload.	5.4	Mo De
CVE-2024-25874	A cross-site scripting (XSS) vulnerability in the New/Edit Article module of Enhavo CMS v0.13.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Create Tag text field.	5.4	Mo De
CVE-2023-43051	IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 267451.	5.4	Mo De
CVE-2024-1758	The SuperFaktura WooCommerce plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.40.3 via the wc_sf_url_check function. This makes it possible for authenticated attackers, with subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	5.4	Mo De
CVE-2024-1687	The Thank You Page Customizer for WooCommerce – Increase Your Sales plugin for WordPress is vulnerable to unauthorized execution of shortcodes due to a missing capability check on the get_text_editor_content() function in all versions up to, and including, 1.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to execute arbitrary shortcodes.	5.4	Mo De
CVE-2024-24099	Code-projects Scholars Tracking System 1.0 is vulnerable to SQL Injection under Employment Status Information Update.	5.4	Mo De
CVE-2024-1672	Inappropriate implementation in Content Security Policy in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	5.4	Mo De
CVE-2024-25905	Cross-Site Request Forgery (CSRF) vulnerability in Mondula GmbH Multi Step Form.This issue affects Multi Step Form: from n/a through 1.7.18.	5.4	Mo De
CVE-2024-25369	A reflected Cross-Site Scripting (XSS) vulnerability in FUEL CMS 1.5.2allows attackers to run arbitrary code via crafted string after the group_id parameter.	5.4	Mo De
CVE-2024-0903	The User Feedback – Create Interactive Feedback Form, User Surveys, and Polls in Seconds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'page_submitted' 'link' value in all versions up to, and including, 1.0.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in the feedback submission page that will execute when a user clicks the link, while also pressing the command key.	5.4	Mo De
CVE-2024-1676	Inappropriate implementation in Navigation in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Low)	5.4	Mo De
CVE-2022-45169	An issue was discovered in LIVEBOX Collaboration vDesk through v031. A URL Redirection to an Untrusted Site (Open Redirect) can occur under the /api/v1/notification/createnotification endpoint, allowing an authenticated user to send an arbitrary push notification to any other user of the system. This push notification can include an (invisible) clickable link.	5.4	Mo De
CVE-2024-26128	baserCMS is a website development framework. Prior to version 5.0.9, there is a cross-site scripting vulnerability in the content management feature. Version 5.0.9 contains a fix for this vulnerability.	5.4	Mo De
CVE-2022-45179	An issue was discovered in LIVEBOX Collaboration vDesk through v031. A basic XSS vulnerability exists under the /api/v1/vdeskintegration/todo/createorupdate endpoint via the title parameter and /dashboard/reminders. A remote user (authenticated to the product) can store arbitrary HTML code in the reminder section title in order to corrupt the web page (for example, by creating phishing sections to exfiltrate victims' credentials).	5.4	Mo De
CVE-2024-26138	The XWiki licensor application, which manages and enforce application licenses for paid extensions, includes the document `Licenses.Code.LicenseJSON` that provides information for admins regarding active licenses. This document is public and thus exposes this information publicly. The information includes the instance's id as well as first and last name and email of the license owner. This is a leak of information that isn't supposed to be public. The instance id allows associating data on the active installs data with the concrete XWiki instance. Active installs assures that "there's no way to find who's having a given UUID" (referring to the instance id). Further, the information who the license owner is and information about the obtained licenses can be used for targeted phishing attacks. Also, while user information is normally public, email addresses might only be displayed obfuscated, depending on the configuration. This has been fixed in Application Licensing 1.24.2. There are no known workarounds besides upgrading.	5.3	Mo De
CVE-2024-24568	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Prior to 7.0.3, the rules inspecting HTTP2 headers can get bypassed by crafted traffic. The vulnerability has been patched in 7.0.3.	5.3	Mo De
CVE-2024-1701	A vulnerability has been found in keerti1924 PHP-MYSQL-User-Login-System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /edit.php. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254389 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-0593	The Simple Job Board plugin for WordPress is vulnerable to unauthorized access of datal due to insufficient authorization checking on the fetch_quick_job() function in all versions up to, and including, 2.10.8. This makes it possible for unauthenticated attackers to fetch arbitrary posts, which can be password protected or private and contain sensitive information.	5.3	Mo De
CVE-2024-24720	An issue was discovered in the Forgot password function in Innovaphone PBX before 14r1 devices. It provides information about whether a user exists on a system.	5.3	Mo De
CVE-2024-1823	A vulnerability classified as critical was found in CodeAstro Simple Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file users.php of the component Backend. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254611.	5.3	Mo De
CVE-2024-0855	The Spiffy Calendar WordPress plugin before 4.9.9 doesn't check the event_author parameter, and allows any user to alter it when creating an event, leading to deceiving users/admins that a page was created by a Contributor+.	5.3	Mo De
CVE-2023-51393	Due to an allocation of resources without limits, an uncontrolled resource consumption vulnerability exists in Silicon Labs Ember ZNet SDK prior to v7.4.0.0 (delivered as part of Silicon Labs Gecko SDK v4.4.0) which may enable attackers to trigger a bus fault and crash of the device, requiring a reboot in order to rejoin the network.	5.3	Mo De
CVE-2024-25896	ChurchCRM 5.5.0 EventEditor.php is vulnerable to Blind SQL Injection (Time-based) via the EID POST parameter.	5.3	Mo De
CVE-2024-1779	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the zt_dcfcf_change_status() function in all versions up to, and including, 1.1.1. This makes it possible for unauthenticated attackers to alter the message read status of messages.	5.3	Mo De
CVE-2023-51394	High traffic environments may result in NULL Pointer Dereference vulnerability in Silicon Labs's Ember ZNet SDK before v7.4.0, causing a system crash.	5.3	Mo De
CVE-2024-26144	Rails is a web-application framework. Starting with version 5.2.0, there is a possible sensitive session information leak in Active Storage. By default, Active Storage sends a Set-Cookie header along with the user's session cookie when serving blobs. It also sets Cache-Control to public. Certain proxies may cache the Set-Cookie, leading to an information leak. The vulnerability is fixed in 7.0.8.1 and 6.1.7.7.	5.3	Mo De
CVE-2024-1525	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Under some specialized conditions, an LDAP user may be able to reset their password using their verified secondary email address and sign-in using direct authentication with the reset password, bypassing LDAP.	5.3	Mo De
CVE-2024-1686	The Thank You Page Customizer for WooCommerce – Increase Your Sales plugin for WordPress is vulnerable to missing authorization e in all versions up to, and including, 1.1.2 via the apply_layout function due to a missing capability check. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve arbitrary order data which may contain PII.	5.3	Mo De
CVE-2021-33146	Improper input validation in some Intel(R) Ethernet Adapters and Intel(R) Ethernet Controller I225 Manageability firmware may allow an unauthenticated user to potentially enable information disclosure via network access.	5.3	Mo De
CVE-2023-42836	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Ventura 13.6.3, macOS Sonoma 14.1, macOS Monterey 12.7.2. An attacker may be able to access connected network volumes mounted in the home directory.	5.3	Mo De
CVE-2023-7033	Insufficient Resource Pool vulnerability in Ethernet function of Mitsubishi Electric Corporation MELSEC iQ-F Series CPU modules allows a remote attacker to cause a temporary Denial of Service condition for a certain period of time in Ethernet communication of the products by performing TCP SYN Flood attack.	5.3	Mo De
CVE-2023-52461	In the Linux kernel, the following vulnerability has been resolved: drm/sched: Fix bounds limiting when given a malformed entity If we're given a malformed entity in drm_sched_entity_init()--shouldn't happen, but we verify--with out-of-bounds priority value, we set it to an allowed value. Fix the expression which sets this limit.	5.3	Mo De
CVE-2024-1899	An issue in the anchors subparser of Showdownjs versions <= 2.1.0 could allow a remote attacker to cause denial of service conditions.	5.3	Mo De
CVE-2024-1436	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wiloke WooCommerce Coupon Popup, SmartBar, Slide In I MyShopKit.This issue affects WooCommerce Coupon Popup, SmartBar, Slide In I MyShopKit: from n/a through 1.0.9.	5.3	Mo De
CVE-2024-21501	Versions of the package sanitize-html before 2.12.1 are vulnerable to Information Exposure when used on the backend and with the style attribute allowed, allowing enumeration of files in the system (including project dependencies). An attacker could exploit this vulnerability to gather details about the file system structure and dependencies of the targeted server.	5.3	Mo De
CVE-2023-30996	IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 could be vulnerable to information leakage due to unverified sources in messages sent between Windows objects of different origins. IBM X-Force ID: 254290.	5.3	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-1562	The WooCommerce Google Sheet Connector plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the execute_post_data function in all versions up to, and including, 1.3.11. This makes it possible for unauthenticated attackers to update plugin settings.	5.3	Mo De
CVE-2024-20325	A vulnerability in the Live Data server of Cisco Unified Intelligence Center could allow an unauthenticated, local attacker to read and modify data in a repository that belongs to an internal service on an affected device. This vulnerability is due to insufficient access control implementations on cluster configuration CLI requests. An attacker could exploit this vulnerability by sending a cluster configuration CLI request to specific directories on an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.	5.1	Mo De
CVE-2024-1748	A vulnerability classified as critical was found in van_der_Schaar LAB AutoPrognosis 0.1.21. This vulnerability affects the function load_model_from_file of the component Release Note Handler. The manipulation leads to deserialization. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-254530 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.0	Mo De
CVE-2024-1925	A vulnerability was found in Ctcms 2.1.2. It has been declared as critical. This vulnerability affects unknown code of the file ctcms/apps/controllers/admin/Upsys.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254860.	5.0	Mo De
CVE-2024-25288	SLIMS (Senayan Library Management Systems) 9 Bulian v9.6.1 is vulnerable to SQL Injection via pop-scope-vocabolary.php.	4.9	Mo De
CVE-2024-25828	cmseasy V7.7.7.9 has an arbitrary file deletion vulnerability in lib/admin/template_admin.php.	4.9	Mo De
CVE-2024-25915	Server-Side Request Forgery (SSRF) vulnerability in Raaj Trambadia Pexels: Free Stock Photos.This issue affects Pexels: Free Stock Photos: from n/a through 1.2.2.	4.9	Mo De
CVE-2024-26302	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager.	4.8	Mo De
CVE-2024-21423	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	4.8	Mo De
CVE-2024-1818	A vulnerability was found in CodeAstro Membership Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /uploads/ of the component Logo Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254606 is the identifier assigned to this vulnerability.	4.7	Mo De
CVE-2024-26281	Upon scanning a JavaScript URI with the QR code scanner, an attacker could have executed unauthorized scripts on the current top origin sites in the URL bar. This vulnerability affects Firefox for iOS < 123.	4.7	Mo De
CVE-2024-26583	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between async notify and socket close The submitting thread (one which called recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete() so any code past that point risks touching already freed data. Try to avoid the locking and extra flags altogether. Have the main thread hold an extra reference, this way we can depend solely on the atomic ref counter for synchronization. Don't futz with reiniting the completion, either, we are now tightly controlling when completion fires.	4.7	Mo De
CVE-2024-22547	WayOS IBR-7150 <17.06.23 is vulnerable to Cross Site Scripting (XSS).	4.7	Mo De
CVE-2024-1819	A vulnerability was found in CodeAstro Membership Management System 1.0. It has been classified as critical. This affects an unknown part of the component Add Members Tab. The manipulation of the argument Member Photo leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254607.	4.7	Mo De
CVE-2024-22776	Wallos 0.9 is vulnerable to Cross Site Scripting (XSS) in all text-based input fields without proper validation, excluding those requiring specific formats like date fields.	4.7	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26152	### Summary On all Label Studio versions prior to 1.11.0, data imported via file upload feature is not properly sanitized prior to being rendered within a [`Choices`](https://labelstud.io/tags/choices) or [`Labels`](https://labelstud.io/tags/labels) tag, resulting in an XSS vulnerability. ### Details Need permission to use the "data import" function. This was reproduced on Label Studio 1.10.1. ### PoC 1. Create a project. ![Create a project](https://github.com/HumanSignal/label-studio/assets/3943358/9b1536ad-feac-4238-a1bd-ca9b1b798673) 2. Upload a file containing the payload using the "Upload Files" function. ![2 Upload a file containing the payload using the Upload Files function](https://github.com/HumanSignal/label-studio/assets/3943358/26bb7af1-1cd2-408f-9adf-61e31a5b7328) ![3 complete](https://github.com/HumanSignal/label-studio/assets/3943358/f2f62774-1fa6-4456-9e6f-8fa1ca0a2d2e) The following are the contents of the files used in the PoC ``` { "data": { "prompt": "labelstudio universe image", "images": [{ "value": "id123#0", "style": "margin: 5px", "html": "<img width='400' src='https://labelstud.io/_astro/images-tab.64279c16_ZaBSvC.avif' onload=alert(document.cookie)>" }] } } ``` 3. Select the text-to-image generation labeling template of Ranking and scoring ![3 Select the text-to-image generation labelling template for Ranking and scoring](https://github.com/HumanSignal/label-studio/assets/3943358/f227f49c-a718-4738-bc2a-807da4f97155) ![5 save](https://github.com/HumanSignal/label-studio/assets/3943358/9b529f8a-8e99-4bb0-bdf6-bb7a95c9b75d) 4. Select a task ![4 Select a task](https://github.com/HumanSignal/label-studio/assets/3943358/71856b7a-2b1f-44ea-99ab-fc48bc20caa7) 5. Check that the script is running ![5 Check that the script is running](https://github.com/HumanSignal/label-studio/assets/3943358/e396ae7b-a591-4db7-afe9-5bab30b48cb9) ### Impact Malicious scripts can be injected into the code, and when linked with vulnerabilities such as CSRF, it can cause even greater damage. In particular, It can become a source of further attacks, especially when linked to social engineering.	4.7	Mo De
CVE-2024-1918	A vulnerability has been found in Byzoro Smart S42 Management Platform up to 20240219 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /useratte/userattestation.php. The manipulation of the argument hidwel leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254839. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	Mo De
CVE-2024-1921	A vulnerability, which was classified as critical, was found in osuuu LightPicture up to 1.2.2. Affected is an unknown function of the file /app/controller/Setup.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254856.	4.7	Mo De
CVE-2021-46925	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix kernel panic caused by race of smc_sock A crash occurs when smc_cdc_tx_handler() tries to access smc_sock but smc_release() has already freed it. [4570.695099] BUG: unable to handle page fault for address: 000000002eae9e88 [4570.696048] #PF: supervisor write access in kernel mode [4570.696728] #PF: error_code(0x0002) - not-present page [4570.697401] PGD 0 P4D 0 [4570.697716] Oops: 0002 [#1] PREEMPT SMP NOPTI [4570.698228] CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.16.0-rc4+ #111 [4570.699013] Hardware name: Alibaba Cloud Alibaba Cloud ECS, BIOS 8c24b4c 04/0 [4570.699933] RIP: 0010:_raw_spin_lock+0x1a/0x30 <...> [4570.711446] Call Trace: [4570.711746] <IRQ> [4570.711992] smc_cdc_tx_handler+0x41/0xc0 [4570.712470] smc_wr_tx_tasklet_fn+0x213/0x560 [4570.712981] ? smc_cdc_tx_dismisser+0x10/0x10 [4570.713489] tasklet_action_common.isra.17+0x66/0x140 [4570.714083] __do_softirq+0x123/0x2f4 [4570.714521] irq_exit_rcu+0xc4/0xf0 [4570.714934] common_interrupt+0xba/0xe0 Though smc_cdc_tx_handler() checked the existence of smc connection, smc_release() may have already dismissed and released the smc socket before smc_cdc_tx_handler() further visits it. smc_cdc_tx_handler() lsmc_release() if (!conn) l l lsmc_cdc_tx_dismiss_slots() l smc_cdc_tx_dismisser() l lsock_put(&smc->sk) <- last sock_put, l smc_sock freed bh_lock_sock(&smc->sk) (panic) l To make sure we won't receive any CDC messages after we free the smc_sock, add a refcount on the smc_connection for inflight CDC message(posted to the QP but haven't received related CQE), and don't release the smc_connection until all the inflight CDC messages haven been done, for both success or failed ones. Using refcount on CDC messages brings another problem: when the link is going to be destroyed, smcr_link_clear() will reset the QP, which then remove all the pending CQEs related to the QP in the CQ. To make sure all the CQEs will always come back so the refcount on the smc_connection can always reach 0, smc_ib_modify_qp_reset() was replaced by smc_ib_modify_qp_error(). And remove the timeout in smc_wr_tx_wait_no_pending_sends() since we need to wait for all pending WQEs done, or we may encounter use-after- free when handling CQEs. For IB device removal routine, we need to wait for all the QPs on that device been destroyed before we can destroy CQs on the device, or the refcount on smc_connection won't reach 0 and smc_sock cannot be released.	4.7	Mo De
CVE-2021-46958	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix race between transaction aborts and fsyncs leading to use-after-free There is a race between a task aborting a transaction during a commit, a task doing an fsync and the transaction kthread, which leads to an use-after-free of the log root tree. When this happens, it results in a stack trace like the following: BTRFS info (device dm-0): forced readonly BTRFS warning (device dm-0): Skipping commit of aborted transaction. BTRFS: error (device dm-0) in cleanup_transaction:1958: errno=-5 IO failure BTRFS warning (device dm-0): lost page write due to IO error on /dev/mapper/error-test (-5) BTRFS warning (device dm-0): Skipping commit of aborted transaction. BTRFS warning (device dm-0): direct IO failed ino 261 rw 0,0 sector 0xa4e8 len 4096 err no 10 BTRFS error (device dm-0): error writing primary super block to device 1 BTRFS warning (device dm-0): direct IO failed ino 261 rw 0,0 sector 0x12e000 len 4096 err no 10 BTRFS warning (device dm-0): direct IO failed ino 261 rw 0,0 sector 0x12e008 len 4096 err no 10 BTRFS warning (device dm-0): direct IO failed ino 261 rw 0,0 sector 0x12e010 len 4096 err no 10 BTRFS: error (device dm-0) in write_all_supers:4110: errno=-5 IO failure (1 errors while writing supers) BTRFS: error (device dm-0) in btrfs_sync_log:3308: errno=-5 IO failure general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6b68: 0000 [#1] PREEMPT SMP DEBUG_PAGEALLOC PTI CPU: 2 PID: 2458471 Comm: fsstress Not tainted 5.12.0-rc5-btrfs-next-84 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 RIP: 0010:__mutex_lock+0x139/0xa40 Code: c0 74 19 (...) RSP: 0018:ffff9f18830d7b00 EFLAGS: 00010202 RAX: 6b6b6b6b6b6b6b68 RBX: 0000000000000001 RCX: 0000000000000002 RDX: ffffffffb9c54d13 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff9f18830d7bc0 R08: 0000000000000000 R09: 0000000000000000 R10: ffff9f18830d7be0 R11: 0000000000000001 R12: ffff8c6cd199c040 R13: ffff8c6c95821358 R14: 00000000fffffffb R15: ffff8c6cbcf01358 FS: 00007fa9140c2b80(0000) GS:ffff8c6fac600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fa913d52000 CR3: 000000013d2b4003 CR4: 0000000000370ee0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: ? __btrfs_handle_fs_error+0xde/0x146 [btrfs] ? btrfs_sync_log+0x7c1/0xf20 [btrfs] ? btrfs_sync_log+0x7c1/0xf20 [btrfs] btrfs_sync_log+0x7c1/0xf20 [btrfs] btrfs_sync_file+0x40c/0x580 [btrfs] do_fsync+0x38/0x70 __x64_sys_fsync+0x10/0x20 do_syscall_64+0x33/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fa9142a55c3 Code: 8b 15 09 (...) RSP: 002b:00007fff26278d48 EFLAGS: 00000246 ORIG_RAX: 000000000000004a RAX: ffffffffffffffda RBX: 0000563c83cb4560 RCX: 00007fa9142a55c3 RDX: 00007fff26278cb0 RSI: 00007fff26278cb0 RDI: 0000000000000005 RBP: 0000000000000005 R08: 0000000000000001 R09: 00007fff26278d5c R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000340 R13: 00007fff26278de0 R14: 00007fff26278d96 R15: 0000563c83ca57c0 Modules linked in: btrfs dm_zero dm_snapshot dm_thin_pool (...) ---[end trace ee2f1b19327d791d]--- The steps that lead to this crash are the following: 1) We are at transaction N; 2) We have two tasks with a transaction handle attached to transaction N. Task A and Task B. Task B is doing an fsync; 3) Task B is at btrfs_sync_log(), and has saved fs_info->log_root_tree into a local variable named 'log_root_tree' at the top of btrfs_sync_log(). Task B is about to call write_all_supers(), but before that... 4) Task A calls btrfs_commit_transaction(), and after it sets the transaction state to TRANS_STATE_COMMIT_START, an error happens before it w ---truncated---	4.7	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-1501	The Database Reset plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.22. This is due to missing or incorrect nonce validation on the install_wpr() function. This makes it possible for unauthenticated attackers to install the WP Reset Plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.7	Mo De
CVE-2024-26585	In the Linux kernel, the following vulnerability has been resolved: tls: fix race between tx work scheduling and socket close Similarly to previous commit, the submitting thread (recvmsg/sendmsg) may exit as soon as the async crypto handler calls complete(). Reorder scheduling the work before calling complete(). This seems more logical in the first place, as it's the inverse order of what the submitting thread will do.	4.7	Mo De
CVE-2024-26481	Kirby CMS v4.1.0 was discovered to contain a reflected self-XSS vulnerability via the URL parameter.	4.7	Mo De
CVE-2024-27087	Kirby is a content management system. The new link field introduced in Kirby 4 allows several different link types that each validate the entered link to the relevant URL format. It also includes a "Custom" link type for advanced use cases that don't fit any of the pre-defined link formats. As the "Custom" link type is meant to be flexible, it also allows the javascript: URL scheme. In some use cases this can be intended, but it can also be misused by attackers to execute arbitrary JavaScript code when a user or visitor clicks on a link that is generated from the contents of the link field. This vulnerability is patched in 4.1.1.	4.6	Mo De
CVE-2024-27093	Minder is a Software Supply Chain Security Platform. In version 0.0.31 and earlier, it is possible for an attacker to register a repository with a invalid or differing upstream ID, which causes Minder to report the repository as registered, but not remediate any future changes which conflict with policy (because the webhooks for the repo do not match any known repository in the database). When attempting to register a repo with a different repo ID, the registered provider must have admin on the named repo, or a 404 error will result. Similarly, if the stored provider token does not have repo access, then the remediations will not apply successfully. Lastly, it appears that reconciliation actions do not execute against repos with this type of mismatch. This appears to primarily be a potential denial-of-service vulnerability. This vulnerability is patched in version 0.20240226.1425+ref.53868a8.	4.6	Mo De
CVE-2024-1590	The Page Builder: Pagelayer – Drag and Drop website builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Button Widget in all versions up to, and including, 1.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.6	Mo De
CVE-2023-42855	This issue was addressed with improved state management. This issue is fixed in iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to silently persist an Apple ID on an erased device.	4.6	Mo De
CVE-2024-27319	Versions of the package onnx before and including 1.15.0 are vulnerable to Out-of-bounds Read as the ONNX_ASSERT and ONNX_ASSERTM functions have an off by one string copy.	4.4	Mo De
CVE-2024-25629	c-ares is a C library for asynchronous DNS requests. `ares__read_line()` is used to parse local configuration files such as `/etc/resolv.conf`, `/etc/nsswitch.conf`, the `HOSTALIASES` file, and if using a c-ares version prior to 1.27.0, the `/etc/hosts` file. If any of these configuration files has an embedded `NULL` character as the first character in a new line, it can lead to attempting to read memory prior to the start of the given buffer which may result in a crash. This issue is fixed in c-ares 1.27.0. No known workarounds exist.	4.4	Mo De
CVE-2023-42952	The issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Ventura 13.6.3, macOS Sonoma 14.1, macOS Monterey 12.7.1. An app with root privileges may be able to access private information.	4.4	Mo De
CVE-2023-49100	Trusted Firmware-A (TF-A) before 2.10 has a potential read out-of-bounds in the SDEI service. The input parameter passed in register x1 is not validated well enough in the function sdei_interrupt_bind. The parameter is passed to a call to plat_ic_get_interrupt_type. It can be any arbitrary value passing checks in the function plat_ic_is_sgi. A compromised Normal World (Linux kernel) can enable a root-privileged attacker to issue arbitrary SMC calls. Using this primitive, he can control the content of registers x0 through x6, which are used to send parameters to TF-A. Out-of-bounds addresses can be read in the context of TF-A (EL3). Because the read value is never returned to non-secure memory or in registers, no leak is possible. An attacker can still crash TF-A, however.	4.4	Mo De
CVE-2024-1649	The Categorify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the categorifyAjaxDeleteCategory function in all versions up to, and including, 1.0.7.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete categories.	4.3	Mo De
CVE-2024-1653	The Categorify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the categorifyAjaxUpdateFolderPosition in all versions up to, and including, 1.0.7.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to update the folder position of categories as well as update the metadata of other taxonomies.	4.3	Mo De
CVE-2024-1906	The Categorify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.7.4. This is due to missing or incorrect nonce validation on the categorifyAjaxAddCategory function. This makes it possible for unauthenticated attackers to add categories via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2024-1652	The Categorify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the categorifyAjaxClearCategory function in all versions up to, and including, 1.0.7.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to clear categories.	4.3	Mo De
CVE-2024-1650	The Categorify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the categorifyAjaxRenameCategory function in all versions up to, and including, 1.0.7.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to rename categories.	4.3	Mo De
CVE-2024-1909	The Categorify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.7.4. This is due to missing or incorrect nonce validation on the categorifyAjaxRenameCategory function. This makes it possible for unauthenticated attackers to rename categories via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-1910	The Categorify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.7.4. This is due to missing or incorrect nonce validation on the categorifyAjaxClearCategory function. This makes it possible for unauthenticated attackers to clear categories via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2024-1912	The Categorify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.7.4. This is due to missing or incorrect nonce validation on the categorifyAjaxUpdateFolderPosition function. This makes it possible for unauthenticated attackers to update the folder position of categories as well as update the metadata of other taxonomies via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2024-1907	The Categorify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.7.4. This is due to missing or incorrect nonce validation on the categorifyAjaxDeleteCategory function. This makes it possible for unauthenticated attackers to delete categories via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2023-50923	In QUIC in RFC 9000, the Latency Spin Bit specification (section 17.4) does not strictly constrain the bit value when the feature is disabled, which might allow remote attackers to construct a covert channel with data represented as changes to the bit value. NOTE: The "Sheridan, S., Keane, A. (2015). In Proceedings of the 14th European Conference on Cyber Warfare and Security (ECCWS), University of Hertfordshire, Hatfield, UK." paper says "Modern Internet communication protocols provide an almost infinite number of ways in which data can be hidden or embed whithin seemingly normal network traffic."	4.3	Mo De
CVE-2024-1165	The Brizy – Page Builder plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.4.39 via the 'id'. This makes it possible for authenticated attackers, with contributor-level access and above, to upload files to arbitrary locations on the server	4.3	Mo De
CVE-2024-24837	Cross-Site Request Forgery (CSRF) vulnerability in Frédéric GILLES FG PrestaShop to WooCommerce, Frédéric GILLES FG Drupal to WordPress, Frédéric GILLES FG Joomla to WordPress.This issue affects FG PrestaShop to WooCommerce: from n/a through 4.44.3; FG Drupal to WordPress: from n/a through 3.67.0; FG Joomla to WordPress: from n/a through 4.15.0.	4.3	Mo De
CVE-2024-0563	Denial of service condition in M-Files Server in versions before 24.2 (excluding 23.2 SR7 and 23.8 SR5) allows anonymous user to cause denial of service against other anonymous users.	4.3	Mo De
CVE-2024-1778	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the zt_dcfcf_change_bookmark() function in all versions up to, and including, 1.1.1. This makes it possible for unauthenticated attackers to alter bookmark statuses.	4.3	Mo De
CVE-2024-1777	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.1. This is due to missing or incorrect nonce validation on the settings update function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2024-24802	Cross-Site Request Forgery (CSRF) vulnerability in John Tendik JTRT Responsive Tables.This issue affects JTRT Responsive Tables: from n/a through 4.1.9.	4.3	Mo De
CVE-2024-24817	Discourse Calendar adds the ability to create a dynamic calendar in the first post of a topic on the open-source discussion platform Discourse. Prior to version 0.4, event invitees created in topics in private categories or PMs (private messages) can be retrieved by anyone, even if they're not logged in. This problem is resolved in version 0.4 of the discourse-calendar plugin. While no known workaround is available, putting the site behind `login_required` will disallow this endpoint to be used by anonymous users, but logged in users can still get the list of invitees in the private topics.	4.3	Mo De
CVE-2024-26349	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/delete_translation.php	4.3	Mo De
CVE-2024-1053	The Event Tickets and Registration plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'email' action in all versions up to, and including, 5.8.1. This makes it possible for authenticated attackers, with contributor-level access and above, to email the attendees list to themselves.	4.3	Mo De
CVE-2024-1361	The Colibri Page Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.253. This is due to missing or incorrect nonce validation on the apiCall() function. This makes it possible for unauthenticated attackers to call a limited set of functions that can be used to import images, delete posts, or save theme data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2023-32344	IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerable to form action hijacking where it is possible to modify the form action to reference an arbitrary path. IBM X-Force ID: 255898.	4.3	Mo De
CVE-2024-26188	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	Mo De
CVE-2023-4895	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 to 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. This vulnerability allows for bypassing the 'group ip restriction' settings to access environment details of projects	4.3	Mo De
CVE-2024-0861	An issue has been discovered in GitLab EE affecting all versions starting from 16.4 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Users with the `Guest` role can change `Custom dashboard projects` settings contrary to permissions.	4.3	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26310	Archer Platform 6.8 before 6.14 P2 (6.14.0.2) contains an improper access control vulnerability. A remote authenticated malicious user could potentially exploit this to gain access to API information that should only be accessible with extra privileges.	4.3	Mo De
CVE-2024-1700	A vulnerability, which was classified as problematic, was found in keerti1924 PHP-MYSQL-User-Login-System 1.0. Affected is an unknown function of the file /signup.php. The manipulation of the argument username with the input <script>alert("xss")</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254388. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	Mo De
CVE-2024-1360	The Colibri WP theme for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.94. This is due to missing or incorrect nonce validation on the colibriwp_install_plugin() function. This makes it possible for unauthenticated attackers to install recommended plugins via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2024-1707	A vulnerability, which was classified as problematic, was found in GARO WALLBOX GLB+ T2EV7 0.5. This affects an unknown part of the file /index.jsp#settings of the component Software Update Handler. The manipulation of the argument Reference leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254397 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	Mo De
CVE-2024-24849	Cross-Site Request Forgery (CSRF) vulnerability in Mark Stockton Quicksand Post Filter jQuery Plugin.This issue affects Quicksand Post Filter jQuery Plugin: from n/a through 3.1.1.	4.3	Mo De
CVE-2024-24872	Cross-Site Request Forgery (CSRF) vulnerability in Themify Themify Builder.This issue affects Themify Builder: from n/a through 7.0.5.	4.3	Mo De
CVE-2023-42843	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1, Safari 17.1, macOS Sonoma 14.1. Visiting a malicious website may lead to address bar spoofing.	4.3	Mo De
CVE-2024-1825	A vulnerability, which was classified as problematic, was found in CodeAstro House Rental Management System 1.0. This affects an unknown part of the component User Registration Page. The manipulation of the argument address with the input <img src="1" onerror="console.log(1)"> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254613 was assigned to this vulnerability.	4.3	Mo De
CVE-2023-42951	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1. A user may be unable to delete browsing history items.	4.3	Mo De
CVE-2024-25770	libming 0.4.8 contains a memory leak vulnerability in /libming/src/actioncompiler/listaction.c.	4.3	Mo De
CVE-2024-1362	The Colibri Page Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.253. This is due to missing or incorrect nonce validation on the cp_shortcode_refresh() function. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	Mo De
CVE-2024-24876	Cross-Site Request Forgery (CSRF) vulnerability in Janis Elsts Admin Menu Editor.This issue affects Admin Menu Editor: from n/a through 1.12.	4.3	Mo De
CVE-2024-25904	Cross-Site Request Forgery (CSRF) vulnerability in David Stockl TinyMCE and TinyMCE Advanced Professsional Formats and Styles.This issue affects TinyMCE and TinyMCE Advanced Professsional Formats and Styles: from n/a through 1.1.2.	4.3	Mo De
CVE-2024-24798	Cross-Site Request Forgery (CSRF) vulnerability in SoniNow Team Debug.This issue affects Debug: from n/a through 1.10.	4.3	Mo De
CVE-2024-25081	Splinefont in FontForge through 20230101 allows command injection via crafted filenames.	4.2	Mo De
CVE-2024-23654	discourse-ai is the AI plugin for the open-source discussion platform Discourse. Prior to commit 94ba0dadc2cf38e8f81c3936974c167219878edd, interactions with different AI services are vulnerable to admin-initiated SSRF attacks. Versions of the plugin that include commit 94ba0dadc2cf38e8f81c3936974c167219878edd contain a patch. As a workaround, one may disable the discourse-ai plugin.	4.1	Mo De
CVE-2024-1784	A vulnerability classified as problematic was found in Limbas 5.2.14. Affected by this vulnerability is an unknown functionality of the file main_admin.php. The manipulation of the argument tab_group leads to sql injection. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254575. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.9	Mo De
CVE-2023-37540	Sametime Connect desktop chat client includes, but does not use or require, the use of an Eclipse feature called Secure Storage. Using this Eclipse feature to store sensitive data can lead to exposure of that data.	3.9	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-26149	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. If an excessively large value is specified as the starting index for an array in `_abi_decode`, it can cause the read position to overflow. This results in the decoding of values outside the intended array bounds, potentially leading to exploitations in contracts that use arrays within `_abi_decode`. This vulnerability affects 0.3.10 and earlier versions.	3.7	Mo De
CVE-2024-24564	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. When using the built-in `extract32(b, start)`, if the `start` index provided has for side effect to update `b`, the byte array to extract `32` bytes from, it could be that some dirty memory is read and returned by `extract32`. This vulnerability is fixed in 0.4.0.	3.7	Mo De
CVE-2023-3509	An issue has been discovered in GitLab affecting all versions before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. It was possible for group members with sub-maintainer role to change the title of privately accessible deploy keys associated with projects in the group.	3.7	Mo De
CVE-2024-1919	A vulnerability classified as problematic was found in SourceCodester Online Job Portal 1.0. This vulnerability affects unknown code of the file /Employer/ManageWalkin.php of the component Manage Walkin Page. The manipulation of the argument Job Title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-254854 is the identifier assigned to this vulnerability.	3.5	Mo De
CVE-2024-1834	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been classified as problematic. This affects an unknown part of the file ?page=attendance&class_id=1. The manipulation of the argument class_date with the input 2024-02-23%22%3E%3Cscript%3Ealert(1)%3C/script%3E leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254625 was assigned to this vulnerability.	3.5	Mo De
CVE-2024-1703	A vulnerability was found in ZhongBangKeJi CRMEB 5.2.2. It has been classified as problematic. This affects the function openfile of the file /adminapi/system/file/openfile. The manipulation leads to absolute path traversal. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254391. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	Mo De
CVE-2024-1922	A vulnerability has been found in SourceCodester Online Job Portal 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /Employer/ManageJob.php of the component Manage Job Page. The manipulation of the argument Qualification/Description leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254857 was assigned to this vulnerability.	3.5	Mo De
CVE-2024-1706	A vulnerability, which was classified as problematic, has been found in ZKTeco ZKBio Access IVS up to 3.3.2. Affected by this issue is some unknown functionality of the component Department Name Search Bar. The manipulation with the input <marquee>hi leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254396. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	Mo De
CVE-2024-1871	A vulnerability, which was classified as problematic, was found in SourceCodester Employee Management System 1.0. Affected is an unknown function of the file /process/assignp.php of the component Project Assignment Report. The manipulation of the argument pname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-254694 is the identifier assigned to this vulnerability.	3.5	Mo De
CVE-2023-42939	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1. A user's private browsing activity may be unexpectedly saved in the App Privacy Report.	3.3	Mo De
CVE-2021-46934	In the Linux kernel, the following vulnerability has been resolved: i2c: validate user data in compat ioctl Wrong user data may cause warning in i2c_transfer(), ex: zero msgs. Userspace should not be able to trigger warnings, so this patch adds validation checks for user data in compact ioctl to prevent reported warnings	3.3	Mo De
CVE-2024-1886	This vulnerability allows remote attackers to traverse the directory on the affected webOS of LG Signage.	3.0	Mo De
CVE-2024-22371	Exposure of sensitive data by by crafting a malicious EventFactory and providing a custom ExchangeCreatedEvent that exposes sensitive data. Vulnerability in Apache Camel.This issue affects Apache Camel: from 3.21.X through 3.21.3, from 3.22.X through 3.22.0, from 4.0.X through 4.0.3, from 4.X through 4.3.0. Users are recommended to upgrade to version 3.21.4, 3.22.1, 4.0.4 or 4.4.0, which fixes the issue.	2.9	Mo De
CVE-2024-25129	The CodeQL CLI repo holds binaries for the CodeQL command line interface (CLI). Prior to version 2.16.3, an XML parser used by the CodeQL CLI to read various auxiliary files is vulnerable to an XML External Entity attack. If a vulnerable version of the CLI is used to process either a maliciously modified CodeQL database, or a specially prepared set of QL query sources, the CLI can be made to make an outgoing HTTP request to an URL that contains material read from a local file chosen by the attacker. This may result in a loss of privacy of exfiltration of secrets. Security researchers and QL authors who receive databases or QL source files from untrusted sources may be impacted. A single untrusted `.ql` or `.qll` file cannot be affected, but a zip archive or tarball containing QL sources may unpack auxiliary files that will trigger an attack when CodeQL sees them in the file system. Those using CodeQL for routine analysis of source trees with a preselected set of trusted queries are not affected. In particular, extracting XML files from a source tree into the CodeQL database does not make one vulnerable. The problem is fixed in release 2.16.3 of the CodeQL CLI. Other than upgrading, workarounds include not accepting CodeQL databases or queries from untrusted sources, or only processing such material on a machine without an Internet connection. Customers who use older releases of CodeQL for security scanning in an automated CI system and cannot upgrade for compliance reasons can continue using that version. That use case is safe. If such customers have a private query pack and use the `codeql pack create` command to precompile them before using them in the CI system, they should be using the production CodeQL release to run `codeql pack create`. That command is safe as long as the QL source it precompiled is trusted. All other development of the query pack should use an upgraded CLI.	2.7	Mo De
CVE-2024-1822	A vulnerability classified as problematic has been found in PHPGurukul Tourism Management System 1.0. Affected is an unknown function of the file user-bookings.php. The manipulation of the argument Full Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-254610 is the identifier assigned to this vulnerability.	2.4	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-1749	A vulnerability, which was classified as problematic, has been found in Bdtask Bhojon Best Restaurant Management Software 2.9. This issue affects some unknown processing of the file /dashboard/message of the component Message Page. The manipulation of the argument Title leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254531. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	Mo De
CVE-2023-50955	IBM InfoSphere Information Server 11.7 could allow an authenticated privileged user to obtain the absolute path of the web server installation which could aid in further attacks against the system. IBM X-Force ID: 275777.	2.4	Mo De
CVE-2023-5775	The BackWPup plugin for WordPress is vulnerable to Plaintext Storage of Backup Destination Password in all versions up to, and including, 4.0.2. This is due to to the plugin improperly storing backup destination passwords in plaintext. This makes it possible for authenticated attackers, with administrator-level access, to retrieve the password from the password input field in the UI or from the options table where the password is stored.	2.2	Mo De
CVE-2024-27088	es5-ext contains ECMAScript 5 extensions. Passing functions with very long names or complex default argument names into `function#copy` or `function#toStringTokens` may cause the script to stall. The vulnerability is patched in v0.10.63.	0.0	Mo De
CVE-2023-48682	Stored cross-site scripting (XSS) vulnerability in unit name. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.	N/A	Mo De
CVE-2023-50380	XML External Entity injection in apache ambari versions <= 2.7.7, Users are recommended to upgrade to version 2.7.8, which fixes this issue. More Details: Oozie Workflow Scheduler had a vulnerability that allowed for root-level file reading and privilege escalation from low-privilege users. The vulnerability was caused through lack of proper user input validation. This vulnerability is known as an XML External Entity (XXE) injection attack. Attackers can exploit XXE vulnerabilities to read arbitrary files on the server, including sensitive system files. In theory, it might be possible to use this to escalate privileges.	N/A	Mo De
CVE-2023-48681	Self cross-site scripting (XSS) vulnerability in storage nodes search field. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.	N/A	Mo De
CVE-2024-24475	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	Mo De
CVE-2024-0763	Any user can delete an arbitrary folder (recursively) on a remote server due to bad input sanitization leading to path traversal. The attacker would need access to the server at some privilege level since this endpoint is protected and requires authorization.	N/A	Mo De
CVE-2024-21742	Improper input validation allows for header injection in MIME4J library when using MIME4J DOM for composing message. This can be exploited by an attacker to add unintended headers to MIME messages.	N/A	Mo De
CVE-2023-48680	Sensitive information disclosure due to excessive collection of system information. The following products are affected: Acronis Cyber Protect 16 (macOS, Windows) before build 37391.	N/A	Mo De
CVE-2023-48679	Stored cross-site scripting (XSS) vulnerability due to missing origin validation in postMessage. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.	N/A	Mo De
CVE-2023-48678	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.	N/A	Mo De
CVE-2024-1866	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2813. Reason: This candidate is a duplicate of CVE-2023-2813. Notes: All CVE users should reference CVE-2023-2813 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	Mo De
CVE-2021-33072	Rejected reason: This is unused.	N/A	Mo De
CVE-2024-1865	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2813. Reason: This candidate is a duplicate of CVE-2023-2813. Notes: All CVE users should reference CVE-2023-2813 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	Mo De
CVE-2024-1864	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2813. Reason: This candidate is a duplicate of CVE-2023-2813. Notes: All CVE users should reference CVE-2023-2813 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	Mo De
CVE-2024-27215	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1709. Reason: This candidate is a duplicate of CVE-2024-1709. Notes: All CVE users should reference CVE-2024-1709 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	Mo De
CVE-2021-46975	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46971	In the Linux kernel, the following vulnerability has been resolved: perf/core: Fix unconditional security_locked_down() call Currently, the lockdown state is queried unconditionally, even though its result is used only if the PERF_SAMPLE_REGS_INTR bit is set in attr.sample_type. While that doesn't matter in case of the Lockdown LSM, it causes trouble with the SELinux's lockdown hook implementation. SELinux implements the locked_down hook with a check whether the current task's type has the corresponding "lockdown" class permission ("integrity" or "confidentiality") allowed in the policy. This means that calling the hook when the access control decision would be ignored generates a bogus permission check and audit record. Fix this by checking sample_type first and only calling the hook when its result would be honored.	N/A	Mo De
CVE-2021-33084	Rejected reason: This is unused.	N/A	Mo De
CVE-2024-25898	A XSS vulnerability was found in the ChurchCRM v.5.5.0 functionality, edit your event, where malicious JS or HTML code can be inserted in the Event Sermon field in EventEditor.php.	N/A	Mo De
CVE-2021-46965	In the Linux kernel, the following vulnerability has been resolved: mtd: physmap: physmap-bt1-rom: Fix unintentional stack access Cast &data to (char *) in order to avoid unintentionally accessing the stack. Notice that data is of type u32, so any increment to &data will be in the order of 4-byte chunks, and this piece of code is actually intended to be a byte offset. Addresses-Coverity-ID: 1497765 ("Out-of-bounds access")	N/A	Mo De
CVE-2024-25249	An issue in He3 App for macOS version 2.0.17, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings.	N/A	Mo De
CVE-2021-46968	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: fix zcard and zqueue hot-unplug memleak Tests with kvm and a kmemdebug kernel showed, that on hot unplug the zcard and zqueue structs for the unplugged card or queue are not properly freed because of a mismatch with get/put for the embedded kref counter. This fix now adjusts the handling of the kref counters. With init the kref counter starts with 1. This initial value needs to drop to zero with the unregister of the card or queue to trigger the release and free the object.	N/A	Mo De
CVE-2021-46969	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: core: Fix invalid error returning in mhi_queue mhi_queue returns an error when the doorbell is not accessible in the current state. This can happen when the device is in non M0 state, like M3, and needs to be waken-up prior ringing the DB. This case is managed earlier by triggering an asynchronous M3 exit via controller resume/suspend callbacks, that in turn will cause M0 transition and DB update. So, since it's not an error but just delaying of doorbell update, there is no reason to return an error. This also fixes a use after free error for skb case, indeed a caller queuing skb will try to free the skb if the queueing fails, but in that case queueing has been done.	N/A	Mo De
CVE-2021-46970	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: pci_generic: Remove WQ_MEM_RECLAIM flag from state workqueue A recent change created a dedicated workqueue for the state-change work with WQ_HIGHPRI (no strong reason for that) and WQ_MEM_RECLAIM flags, but the state-change work (mhi_pm_st_worker) does not guarantee forward progress under memory pressure, and will even wait on various memory allocations when e.g. creating devices, loading firmware, etc... The work is then not part of a memory reclaim path... Moreover, this causes a warning in check_flush_dependency() since we end up in code that flushes a non-reclaim workqueue: [40.969601] workqueue: WQ_MEM_RECLAIM mhi_hiprio_wq:mhi_pm_st_worker [mhi] is flushing !WQ_MEM_RECLAIM events_highpri:flush_backlog [40.969612] WARNING: CPU: 4 PID: 158 at kernel/workqueue.c:2607 check_flush_dependency+0x11c/0x140 [40.969733] Call Trace: [40.969740] __flush_work+0x97/0x1d0 [40.969745] ? wake_up_process+0x15/0x20 [40.969749] ? insert_work+0x70/0x80 [40.969750] ? __queue_work+0x14a/0x3e0 [40.969753] flush_work+0x10/0x20 [40.969756] rollback_registered_many+0x1c9/0x510 [40.969759] unregister_netdevice_queue+0x94/0x120 [40.969761] unregister_netdev+0x1d/0x30 [40.969765] mhi_net_remove+0x1a/0x40 [mhi_net] [40.969770] mhi_driver_remove+0x124/0x250 [mhi] [40.969776] device_release_driver_internal+0xf0/0x1d0 [40.969778] device_release_driver+0x12/0x20 [40.969782] bus_remove_device+0xe1/0x150 [40.969786] device_del+0x17b/0x3e0 [40.969791] mhi_destroy_device+0x9a/0x100 [mhi] [40.969796] ? mhi_unmap_single_use_bb+0x50/0x50 [mhi] [40.969799] device_for_each_child+0x5e/0xa0 [40.969804] mhi_pm_st_worker+0x921/0xf50 [mhi]	N/A	Mo De
CVE-2024-25801	SKINsoft S-Museum 7.02.3 allows XSS via the filename of an uploaded file. Unlike in CVE-2024-25802, the attack payload is in the name (not the content) of a file.	N/A	Mo De
CVE-2021-46964	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Reserve extra IRQ vectors Commit a6dcfe08487e ("scsi: qla2xxx: Limit interrupt vectors to number of CPUs") lowers the number of allocated MSI-X vectors to the number of CPUs. That breaks vector allocation assumptions in qla83xx_iospace_config(), qla24xx_enable_msix() and qla2x00_iospace_config(). Either of the functions computes maximum number of qpairs as: ha->max_qpairs = ha->msix_count - 1 (MB interrupt) - 1 (default response queue) - 1 (ATIO, in dual or pure target mode) max_qpairs is set to zero in case of two CPUs and initiator mode. The number is then used to allocate ha->queue_pair_map inside qla2x00_alloc_queues(). No allocation happens and ha->queue_pair_map is left NULL but the driver thinks there are queue pairs available. qla2xxx_queuecommand() tries to find a qpair in the map and crashes: if (ha->mqenable) { uint32_t tag; uint16_t hwq; struct qla_qpair *qpair = NULL; tag = blk_mq_unique_tag(cmd->request); hwq = blk_mq_unique_tag_to_hwq(tag); qpair = ha->queue_pair_map[hwq]; # <- HERE if (qpair) return qla2xxx_mqueuecommand(host, cmd, qpair); } BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 0 PID: 72 Comm: kworker/u4:3 Tainted: G W 5.10.0-rc1+ #25 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.0.0-prebuilt.qemu-project.org 04/01/2014 Workqueue: scsi_wq_7 fc_scsi_scan_rport [scsi_transport_fc] RIP: 0010:qla2xxx_queuecommand+0x16b/0x3f0 [qla2xxx] Call Trace: scsi_queue_rq+0x58c/0xa60 blk_mq_dispatch_rq_list+0x2b7/0x6f0 ? __sbitmap_get_word+0x2a/0x80 __blk_mq_sched_dispatch_requests+0xb8/0x170 blk_mq_sched_dispatch_requests+0x2b/0x50 __blk_mq_run_hw_queue+0x49/0xb0 __blk_mq_delay_run_hw_queue+0xfb/0x150 blk_mq_sched_insert_request+0xbe/0x110 blk_execute_rq+0x45/0x70 __scsi_execute+0x10e/0x250 scsi_probe_and_add_lun+0x228/0xda0 __scsi_scan_target+0xf4/0x620 ? __pm_runtime_resume+0x4f/0x70 scsi_scan_target+0x100/0x110 fc_scsi_scan_rport+0xa1/0xb0 [scsi_transport_fc] process_one_work+0x1ea/0x3b0 worker_thread+0x28/0x3b0 ? process_one_work+0x3b0/0x3b0 kthread+0x112/0x130 ? kthread_park+0x80/0x80 ret_from_fork+0x22/0x30 The driver should allocate enough vectors to provide every CPU it's own HW queue and still handle reserved (MB, RSP, ATIO) interrupts. The change fixes the crash on dual core VM and prevents unbalanced QP allocation where nr_hw_queues is two less than the number of CPUs.	N/A	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-46972	In the Linux kernel, the following vulnerability has been resolved: ovl: fix leaked dentry Since commit 6815f479ca90 ("ovl: use only uppermetacopy state in ovl_lookup()"), overlayfs doesn't put temporary dentry when there is a metacopy error, which leads to dentry leaks when shutting down the related superblock: overlayfs: refusing to follow metacopy origin for (/file0) ... BUG: Dentry (____ptrval____){i=3f33,n=file3} still in use (1) [unmount of overlay overlay] ... WARNING: CPU: 1 PID: 432 at umount_check.cold+0x107/0x14d CPU: 1 PID: 432 Comm: unmount-overlay Not tainted 5.12.0-rc5 #1 ... RIP: 0010:umount_check.cold+0x107/0x14d ... Call Trace: d_walk+0x28c/0x950 ? dentry_lru_isolate+0x2b0/0x2b0 ? __kasan_slab_free+0x12/0x20 do_one_tree+0x33/0x60 shrink_dcache_for_umount+0x78/0x1d0 generic_shutdown_super+0x70/0x440 kill_anon_super+0x3e/0x70 deactivate_locked_super+0xc4/0x160 deactivate_super+0xfa/0x140 cleanup_mnt+0x22e/0x370 __cleanup_mnt+0x1a/0x30 task_work_run+0x139/0x210 do_exit+0xb0c/0x2820 ? __kasan_check_read+0x1d/0x30 ? find_held_lock+0x35/0x160 ? lock_release+0x1b6/0x660 ? mm_update_next_owner+0xa20/0xa20 ? reacquire_held_locks+0x3f0/0x3f0 ? __sanitizer_cov_trace_const_cmp4+0x22/0x30 do_group_exit+0x135/0x380 __do_sys_exit_group.isra.0+0x20/0x20 __x64_sys_exit_group+0x3c/0x50 do_syscall_64+0x45/0x70 entry_SYSCALL_64_after_hwframe+0x44/0xae ... VFS: Busy inodes after unmount of overlay. Self-destruct in 5 seconds. Have a nice day... This fix has been tested with a syzkaller reproducer.	N/A	Mo De
CVE-2024-26489	A cross-site scripting (XSS) vulnerability in the Addon JD Flusity 'Social block links' module of flusity-CMS v2.33 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Profile Name text field.	N/A	Mo De
CVE-2024-26287	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	Mo De
CVE-2021-46946	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	Mo De
CVE-2024-26350	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/update_contact_form_settings.php	N/A	Mo De
CVE-2024-1563	An attacker could have executed unauthorized scripts on top origin sites using a JavaScript URI when opening an external URL with a custom Firefox scheme and a timeout race condition. This vulnerability affects Focus for iOS < 122.	N/A	Mo De
CVE-2021-46974	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix masking negation logic upon negative dst register The negation logic for the case where the off_reg is sitting in the dst register is not correct given then we cannot just invert the add to a sub or vice versa. As a fix, perform the final bitwise and-op unconditionally into AX from the off_reg, then move the pointer from the src to dst and finally use AX as the source for the original pointer arithmetic operation such that the inversion yields a correct result. The single non-AX mov in between is possible given constant blinding is retaining it as it's not an immediate based operation.	N/A	Mo De
CVE-2024-26464	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	Mo De
CVE-2024-25248	SQL Injection vulnerability in the orderGoodsDelivery() function in Niushop B2B2C V5 allows attackers to run arbitrary SQL commands via the order_id parameter.	N/A	Mo De
CVE-2021-33085	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41859	Rejected reason: This is unused.	N/A	Mo De
CVE-2023-7115	The Page Builder: Pagelayer WordPress plugin before 1.8.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	Mo De
CVE-2023-7198	The WP Dashboard Notes WordPress plugin before 1.0.11 is vulnerable to Insecure Direct Object References (IDOR) in post_id= parameter. Authenticated users are able to delete private notes associated with different user accounts. This poses a significant security risk as it violates the principle of least privilege and compromises the integrity and privacy of user data.	N/A	Mo De
CVE-2024-24681	An issue was discovered in Yealink Configuration Encrypt Tool (AES version) and Yealink Configuration Encrypt Tool (RSA version before 1.2). There is a single hardcoded key (used to encrypt provisioning documents) across customers' installations.	N/A	Mo De
CVE-2021-44457	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-43351	Rejected reason: This is unused.	N/A	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-41860	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41858	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-3885	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41857	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41856	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41855	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41854	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41853	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-41852	Rejected reason: This is unused.	N/A	Mo De
CVE-2023-52466	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	Mo De
CVE-2024-0243	With the following crawler configuration: ```python from bs4 import BeautifulSoup as Soup url = "https://example.com" loader = RecursiveUrlLoader(url=url, max_depth=2, extractor=lambda x: Soup(x, "html.parser").text) docs = loader.load() ``` An attacker in control of the contents of `https://example.com` could place a malicious HTML file in there with links like "https://example.completely.different/my_file.html" and the crawler would proceed to download that file as well even though `prevent_outside=True`. https://github.com/langchain-ai/langchain/blob/bf0b3cc0b5ade1fb95a5b1b6fa260e99064c2e22/libs/community/langchain_community/document_loaders/recursive_url_loader.py#L51-L51 Resolved in https://github.com/langchain-ai/langchain/pull/15559	N/A	Mo De
CVE-2024-0435	User can send a chat that contains an XSS opportunity that will then run when the chat is sent and on subsequent page loads. Given the minimum requirement for a user to send a chat is to be given access to a workspace via an admin the risk is low. Additionally, the location in which the XSS renders is only limited to the user who submits the XSS. Ultimately, this attack is limited to the user attacking themselves. There is no anonymous chat submission unless the user does not take the minimum steps required to protect their instance.	N/A	Mo De
CVE-2024-0436	Theoretically, it would be possible for an attacker to brute-force the password for an instance in single-user password protection mode via a timing attack given the linear nature of the `!==` used for comparison. The risk is minified by the additional overhead of the request, which varies in a non-constant nature making the attack less reliable to execute	N/A	Mo De
CVE-2024-0439	As a manager, you should not be able to modify a series of settings. In the UI this is indeed hidden as a convenience for the role since most managers would not be savvy enough to modify these settings. They can use their token to still modify those settings though through a standard HTTP request While this is not a critical vulnerability, it does indeed need to be patched to enforce the expected permission level.	N/A	Mo De
CVE-2024-0440	Attacker, with permission to submit a link or submits a link via POST to be collected that is using the file:// protocol can then introspect host files and other relatively stored files.	N/A	Mo De
CVE-2024-0455	The inclusion of the web scraper for AnythingLLM means that any user with the proper authorization level (manager, admin, and when in single user) could put in the URL ``` http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance ``` which is a special IP and URL that resolves only when the request comes from within an EC2 instance. This would allow the user to see the connection/secret credentials for their specific instance and be able to manage it regardless of who deployed it. The user would have to have pre-existing knowledge of the hosting infra which the target instance is deployed on, but if sent - would resolve if on EC2 and the proper `iptable` or firewall rule is not configured for their setup.	N/A	Mo De
CVE-2024-0798	A privilege escalation vulnerability exists in mintplex-labs/anything-llm, allowing users with 'default' role to delete documents uploaded by 'admin'. Despite the intended restriction that prevents 'default' role users from deleting admin-uploaded documents, an attacker can exploit this vulnerability by sending a crafted DELETE request to the /api/system/remove-document endpoint. This vulnerability is due to improper access control checks, enabling unauthorized document deletion and potentially leading to loss of data integrity.	N/A	Mo De

CVE Number	Description	Base Score	Re
CVE-2024-25760	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	Mo De
CVE-2024-24402	An issue in Nagios XI 2024R1.01 allows a remote attacker to escalate privileges via a crafted script to the /usr/local/nagios/bin/npcd component.	N/A	Mo De
CVE-2021-46907	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	Mo De
CVE-2019-25161	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	Mo De
CVE-2024-0759	Should an instance of AnythingLLM be hosted on an internal network and the attacked be explicitly granted a permission level of manager or admin, they could link-scrape internally resolving IPs of other services that are on the same network as AnythingLLM. This would require the attacker also be able to guess these internal IPs as `/*` ranging is not possible, but could be brute forced. There is a duty of care that other services on the same network would not be fully open and accessible via a simple CuRL with zero authentication as it is not possible to set headers or access via the link collector.	N/A	Mo De
CVE-2024-27084	Rejected reason: This CVE is a duplicate of CVE-2024-1631.	N/A	Mo De
CVE-2024-25711	diffoscope before 256 allows directory traversal via an embedded filename in a GPG file. Contents of any file, such as ../.ssh/id_rsa, may be disclosed to an attacker. This occurs because the value of the gpg --use-embedded-filenames option is trusted.	N/A	Mo De
CVE-2024-24100	Code-projects Computer Book Store 1.0 is vulnerable to SQL Injection via PublisherID.	N/A	Mo De
CVE-2024-24528	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	Mo De
CVE-2021-41851	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-37405	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33099	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33116	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33127	Rejected reason: This is unused.	N/A	Mo De
CVE-2024-0551	Enable exports of the database and associated exported information of the system via the default user role. The attacked would have to have been granted access to the system prior to the attack. It is worth noting that the deterministic nature of the export name is lower risk as the UI for exporting would start the download at the same time, which once downloaded - deletes the export from the system. The endpoint for exporting should simply be patched to a higher privilege level.	N/A	Mo De
CVE-2021-33125	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33121	Rejected reason: This is unused.	N/A	Mo De
CVE-2023-5947	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-7247. Reason: This candidate is a duplicate of CVE-2023-7247. Notes: All CVE users should reference CVE-2023-7247 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	Mo De
CVE-2024-1423	Rejected reason: Accidental Request	N/A	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-33112	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33167	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33111	Rejected reason: This is unused.	N/A	Mo De
CVE-2024-27089	Rejected reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not in the allowed scope of that CNA's CVE ID assignments.	N/A	Mo De
CVE-2021-33109	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33102	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33100	Rejected reason: This is unused.	N/A	Mo De
CVE-2024-25400	Subrion CMS 4.2.1 is vulnerable to SQL Injection via ia.core.mysqli.php. NOTE: this is disputed by multiple third parties because it refers to an HTTP request to a PHP file that only contains a class, without any mechanism for accepting external input, and the reportedly vulnerable method is not present in the file.	N/A	Mo De
CVE-2021-33131	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33132	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33133	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33134	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33136	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33138	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33143	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33144	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33148	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33151	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33152	Rejected reason: This is unused.	N/A	Mo De

CVE Number	Description	Base Score	Re
CVE-2021-33153	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33154	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33156	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33160	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33163	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33165	Rejected reason: This is unused.	N/A	Mo De
CVE-2021-33140	Rejected reason: This is unused.	N/A	Mo De