SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 August 2021

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-2021-32798	The Jupyter notebook is a web-based notebook environment for interactive computing. In affected versions untrusted notebook can execute code on load. Jupyter Notebook uses a deprecated version of Google Caja to sanitize user inputs. A public Caja bypass can be used to trigger an XSS when a victim opens a malicious ipynb document in Jupyter Notebook. The XSS allows an attacker to execute arbitrary code on the victim computer using Jupyter APIs.	10.0	More Details
CVE-2021-32590	Multiple improper neutralization of special elements used in an SQL command vulnerabilities in FortiPortal 6.0.0 through 6.0.4, 5.3.0 through 5.3.5, 5.2.0 through 5.2.5, and 4.2.2 and earlier may allow an attacker with regular user's privileges to execute arbitrary commands on the underlying SQL database via specifically crafted HTTP requests.	9.9	More Details
CVE-2021-38197	unarr.go in go-unarr (aka Go bindings for unarr) 0.1.1 allows Directory Traversal via ../ in a pathname within a TAR archive.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36434	An issue was discovered in the sys-info crate before 0.8.0 for Rust. sys_info::disk_info calls can trigger a double free.	9.8	More Details
CVE-2020-36443	An issue was discovered in the libp2p-deflate crate before 0.27.1 for Rust. An uninitialized buffer is passed to AsyncRead::poll_read(), which is a user-provided trait function.	9.8	More Details
CVE-2020-36452	An issue was discovered in the array-tools crate before 0.3.2 for Rust. FixedCapacityDequeLike::clone() has a drop of uninitialized memory.	9.8	More Details
CVE-2021-38187	An issue was discovered in the anymap crate through 0.12.1 for Rust. It violates soundness via conversion of a *u8 to a *u64.	9.8	More Details
CVE-2021-38188	An issue was discovered in the iced-x86 crate through 1.10.3 for Rust. In Decoder::new(), slice.get_unchecked(slice.length()) is used unsafely.	9.8	More Details
CVE-2021-38189	An issue was discovered in the lettre crate before 0.9.6 for Rust. In an e-mail message body, an attacker can place a . character after two <CR> <LF> sequences and then inject arbitrary SMTP commands.	9.8	More Details
CVE-2021-38190	An issue was discovered in the nalgebra crate before 0.27.1 for Rust. It allows out-of-bounds memory access because it does not ensure that the number of elements is equal to the product of the row count and column count.	9.8	More Details
CVE-2021-38194	An issue was discovered in the ark-r1cs-std crate before 0.3.1 for Rust. It does not enforce any constraints in the FieldVar::mul_by_inverse method. Thus, a prover can produce a proof that is unsound but is nonetheless verified.	9.8	More Details
CVE-2021-38195	An issue was discovered in the libsecp256k1 crate before 0.5.0 for Rust. It can verify an invalid signature because it allows the R or S parameter to be larger than the curve order, aka an overflow.	9.8	More Details
CVE-2021-38196	An issue was discovered in the better-macro crate through 2021-07-22 for Rust. It intentionally demonstrates that remote attackers can execute arbitrary code via proc-macros, and otherwise has no legitimate purpose.	9.8	More Details
CVE-2021-37232	A stack overflow vulnerability occurs in Atomicparsley 20210124.204813.840499f through APar_read64() in src/util.cpp due to the lack of buffer size of uint32_buffer while reading more bytes in APar_read64.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38173	Btrbk before 0.31.2 allows command execution because of the mishandling of remote hosts filtering SSH commands using ssh_filter_btrbk.sh in authorized_keys.	9.8	More Details
CVE-2021-24507	The Astra Pro Addon WordPress plugin before 3.5.2 did not properly sanitise or escape some of the POST parameters from the astra_pagination_infinite and astra_shop_pagination_infinite AJAX action (available to both unauthenticated and authenticated user) before using them in SQL statement, leading to an SQL Injection issues	9.8	More Details
CVE-2021-22910	A sanitization vulnerability exists in Rocket.Chat server versions <3.13.2, <3.12.4, <3.11.4 that allowed queries to an endpoint which could result in a NoSQL injection, potentially leading to RCE.	9.8	More Details
CVE-2013-6276	QNAP F_VioCard 2312 and F_VioGate 2308 have hardcoded entries in authorized_keys files. NOTE: 1. All active models are not affected. The last affected model was EOL since 2010. 2. The legacy authorization mechanism is no longer adopted in all active models	9.8	More Details
CVE-2014-9320	SAP BusinessObjects Edge 4.1 allows remote attackers to obtain the SI_PLATFORM_SEARCH_SERVER_LOGON_TOKEN token and consequently gain SYSTEM privileges via vectors involving CORBA calls, aka SAP Note 2039905.	9.8	More Details
CVE-2021-21564	Dell OpenManage Enterprise versions prior to 3.6.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to hijack an elevated session or perform unauthorized actions by sending malformed data.	9.8	More Details
CVE-2020-23151	rConfig 3.9.5 allows command injection by sending a crafted GET request to lib/ajaxHandlers/ajaxArchiveFiles.php since the path parameter is passed directly to the exec function without being escaped.	9.8	More Details
CVE-2021-32943	The affected product is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code on the WebAccess/SCADA (WebAccess/SCADA versions prior to 8.4.5, WebAccess/SCADA versions prior to 9.0.1).	9.8	More Details
CVE-2021-38140	The set_user extension module before 2.0.1 for PostgreSQL allows a potential privilege escalation using RESET SESSION AUTHORIZATION after set_user().	9.8	More Details
CVE-2021-38383	OwnTone (aka owntone-server) through 28.1 has a use-after-free in net_bind() in misc.c.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38384	Serverless Offline 8.0.0 returns a 403 HTTP status code for a route that has a trailing / character, which might cause a developer to implement incorrect access control, because the actual behavior within the Amazon AWS environment is a 200 HTTP status code (i.e., possibly greater than expected permissions).	9.8	More Details
CVE-2021-24499	The Workreap WordPress theme before 2.2.2 AJAX actions workreap_award_temp_file_uploader and workreap_temp_file_uploader did not perform nonce checks, or validate that the request is from a valid user in any other way. The endpoints allowed for uploading arbitrary files to the uploads/workreap-temp directory. Uploaded files were neither sanitized nor validated, allowing an unauthenticated visitor to upload executable code such as php scripts.	9.8	More Details
CVE-2020-36432	An issue was discovered in the alg_ds crate through 2020-08-25 for Rust. There is a drop of uninitialized memory in Matrix::new().	9.8	More Details
CVE-2021-38167	Roxy-WI through 5.2.2.0 allows SQL Injection via check_login. An unauthenticated attacker can extract a valid uuid to bypass authentication.	9.8	More Details
CVE-2021-36209	In JetBrains Hub before 2021.1.13389, account takeover was possible during password reset.	9.8	More Details
CVE-2021-1609	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-1610	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2021-20028	Improper neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29971	If a user had granted a permission to a webpage and saved that grant, any webpage running on the same host - irrespective of scheme or port - would be granted that permission. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 90.	9.8	More Details
CVE-2021-29978	Multiple low security issues were discovered and fixed in a security audit of Mozilla VPN 2.x branch as part of a 3rd party security audit. This vulnerability affects Mozilla VPN < 2.3.	9.8	More Details
CVE-2021-34371	Neo4j through 3.4.18 (with the shell server enabled) exposes an RMI service that arbitrarily deserializes Java objects, e.g., through setSessionVariable. An attacker can abuse this for remote code execution because there are dependencies with exploitable gadget chains.	9.8	More Details
CVE-2021-21805	An OS Command Injection vulnerability exists in the ping.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). A specially crafted HTTP request can lead to arbitrary OS command execution. An attacker can send a crafted HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-35324	A vulnerability in the Form_Login function of TOTOLINK A720R A720R_Firmware V4.1.5cu.470_B20200911 allows attackers to bypass authentication.	9.8	More Details
CVE-2021-35327	A vulnerability in TOTOLINK A720R A720R_Firmware v4.1.5cu.470_B20200911 allows attackers to start the Telnet service, then login with the default credentials via a crafted POST request.	9.8	More Details
CVE-2021-38159	In certain Progress MOVEit Transfer versions before 2021.0.4 (aka 13.0.4), SQL injection in the MOVEit Transfer web application could allow an unauthenticated remote attacker to gain access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, or execute SQL statements that alter or delete database elements, via crafted strings sent to unique MOVEit Transfer transaction types. The fixed versions are 2019.0.8 (11.0.8), 2019.1.7 (11.1.7), 2019.2.4 (11.2.4), 2020.0.7 (12.0.7), 2020.1.6 (12.1.6), and 2021.0.4 (13.0.4).	9.8	More Details
CVE-2021-37388	A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping_ipaddr parameter in ping_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution.	9.8	More Details
CVE-2021-36351	SQL Injection Vulnerability in Care2x Open Source Hospital Information Management 2.7 Alpha via the (1) pday, (2) pmonth, and (3) pyear parameters in GET requests sent to /modules/nursing/nursing-station.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36705	In ProLink PRC2402M V1.0.18 and older, the set_TR069 function in the adm.cgi binary, accessible with a page parameter value of TR069 contains a trivial command injection where the value of the TR069_local_port parameter is passed directly to system.	9.8	More Details
CVE-2021-36706	In ProLink PRC2402M V1.0.18 and older, the set_sys_cmd function in the adm.cgi binary, accessible with a page parameter value of sysCMD contains a trivial command injection where the value of the command parameter is passed directly to system.	9.8	More Details
CVE-2021-36707	In ProLink PRC2402M V1.0.18 and older, the set_ledonoff function in the adm.cgi binary, accessible with a page parameter value of ledonoff contains a trivial command injection where the value of the led_cmd parameter is passed directly to do_system.	9.8	More Details
CVE-2021-37544	In JetBrains TeamCity before 2020.2.4, there was an insecure deserialization.	9.8	More Details
CVE-2021-26606	A vulnerability in PKI Security Solution of Dream Security could allow arbitrary command execution. This vulnerability is due to insufficient validation of the authorization certificate. An attacker could exploit this vulnerability by sending a crafted HTTP request an affected program. A successful exploit could allow the attacker to remotely execute arbitrary code on a target system.	9.8	More Details
CVE-2020-28088	An arbitrary file upload vulnerability in /jeecg-boot/sys/common/upload of jeecg-boot CMS 2.3 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-38148	Obsidian before 0.12.12 does not require user confirmation for non-http/https URLs.	9.8	More Details
CVE-2021-20032	SonicWall Analytics 2.5 On-Prem is vulnerable to Java Debug Wire Protocol (JDWP) interface security misconfiguration vulnerability which potentially leads to Remote Code Execution. This vulnerability impacts Analytics On-Prem 2.5.2518 and earlier.	9.8	More Details
CVE-2021-22234	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.11 before 13.11.7, all versions starting from 13.12 before 13.12.8, and all versions starting from 14.0 before 14.0.4. A specially crafted design image allowed attackers to read arbitrary files on the server.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21596	Dell OpenManage Enterprise versions 3.4 through 3.6.1 and Dell OpenManage Enterprise Modular versions 1.20.00 through 1.30.00, contain a remote code execution vulnerability. A malicious attacker with access to the immediate subnet may potentially exploit this vulnerability leading to information disclosure and a possible elevation of privileges.	9.6	More Details
CVE-2021-21585	Dell OpenManage Enterprise versions prior to 3.6.1 contain an OS command injection vulnerability in RACADM and IPMI tools. A remote authenticated malicious user with high privileges may potentially exploit this vulnerability to execute arbitrary OS commands.	9.1	More Details
CVE-2021-37549	In JetBrains YouTrack before 2021.1.11111, sandboxing in workflows was insufficient.	9.1	More Details
CVE-2021-20597	Insufficiently Protected Credentials vulnerability in Mitsubishi Electric MELSEC iQ-R series Safety CPU modules R08/16/32/120SFCPU firmware versions "26" and prior and Mitsubishi Electric MELSEC iQ-R series SIL2 Process CPU modules R08/16/32/120PSFCPU firmware versions "11" and prior allows a remote unauthenticated attacker to login to the target unauthorizedly by sniffing network traffic and obtaining credentials when registering user information in the target or changing a password.	9.1	More Details
CVE-2021-29922	library/std/src/net/parser.rs in Rust before 1.53.0 does not properly consider extraneous zero characters at the beginning of an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses, because of unexpected octal interpretation.	9.1	More Details
CVE-2021-37425	Altova MobileTogether Server before 7.3 SP1 allows XXE attacks, such as an InfoSetChanges/Changes attack against /workflowmanagement, or reading mobiletogetherserver.cfg and then reading the certificate and private key.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2013-4717	Multiple SQL injection vulnerabilities in Open Ticket Request System (OTRS) Help Desk 3.0.x before 3.0.22, 3.1.x before 3.1.18, and 3.2.x before 3.2.9 allow remote authenticated users to execute arbitrary SQL commands via unspecified vectors related to Kernel/Output/HTML/PreferencesCustomQueue.pm, Kernel/System/CustomerCompany.pm, Kernel/System/Ticket/IndexAccelerator/RuntimeDB.pm, Kernel/System/Ticket/IndexAccelerator/StaticDB.pm, and Kernel/System/TicketSearch.pm.	8.8	More Details
CVE-2021-36455	SQL Injection vulnerability in Naviwebs Navigate CMS 2.9 via the quicksearch parameter in \lib\packages\comments\comments.php.	8.8	More Details
CVE-2021-37614	In certain Progress MOVEit Transfer versions before 2021.0.3 (aka 13.0.3), SQL injection in the MOVEit Transfer web application could allow an authenticated remote attacker to gain access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, or execute SQL statements that alter or delete database elements, via crafted strings sent to unique MOVEit Transfer transaction types. The fixed versions are 2019.0.7 (11.0.7), 2019.1.6 (11.1.6), 2019.2.3 (11.2.3), 2020.0.6 (12.0.6), 2020.1.5 (12.1.5), and 2021.0.3 (13.0.3).	8.8	More Details
CVE-2021-34634	The Nifty Newsletters WordPress plugin is vulnerable to Cross-Site Request Forgery via the sola_nl_wp_head function found in the ~/sola-newsletters.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.0.23.	8.8	More Details
CVE-2020-7863	A vulnerability in File Transfer Solution of Raonwiz could allow arbitrary command execution as the result of viewing a specially-crafted web page. This vulnerability is due to insufficient validation of the parameter of the specific method. An attacker could exploit this vulnerability by setting the parameter to the command they want to execute. A successful exploit could allow the attacker to execute arbitrary commands on a target system as the user. However, the victim must run the Internet Explorer browser with administrator privileges because of the cross-domain policy.	8.8	More Details
CVE-2020-29011	Instances of SQL Injection vulnerabilities in the checksum search and MTA-quarantine modules of FortiSandbox 3.2.0 through 3.2.2, and 3.1.0 through 3.1.4 may allow an authenticated attacker to execute unauthorized code on the underlying SQL interpreter via specifically crafted HTTP requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26097	An improper neutralization of special elements used in an OS Command vulnerability in FortiSandbox 3.2.0 through 3.2.2, 3.1.0 through 3.1.4, and 3.0.0 through 3.0.6 may allow an authenticated attacker with access to the web GUI to execute unauthorized code or commands via specifically crafted HTTP requests.	8.8	More Details
CVE-2021-21601	Dell EMC Data Protection Search, 19.4 and prior, and IDPA, 2.6.1 and prior, contain an Information Exposure in Log File Vulnerability in CIS. A local low privileged attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with the privileges of the compromised account.	8.8	More Details
CVE-2021-33256	A CSV injection vulnerability on the login panel of ManageEngine ADSelfService Plus Version: 6.1 Build No: 6101 can be exploited by an unauthenticated user. The j_username parameter seems to be vulnerable and a reverse shell could be obtained if a privileged user exports "User Attempts Audit Report" as CSV file. Note: The vendor disputes this vulnerability, claiming "This is not a valid vulnerability in our ADSSP product. We don't see this as a security issue at our side.	8.8	More Details
CVE-2021-32465	An incorrect permission preservation vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a remote user to perform an attack and bypass authentication on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	8.8	More Details
CVE-2021-37214	The employee management page of Flygo contains Insecure Direct Object Reference (IDOR) vulnerability. After being authenticated as a general user, remote attackers can manipulate the employee ID in specific parameters to arbitrary access employee's data, modify it, and then obtain administrator privilege and execute arbitrary command.	8.8	More Details
CVE-2021-21831	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software’s PDF Reader, version 10.1.3.37598. A specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2021-38111	The DEF CON 27 badge allows remote attackers to exploit a buffer overflow by sending an oversized packet via the NFMI (Near Field Magnetic Induction) protocol.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37543	In JetBrains RubyMine before 2021.1.1, code execution without user confirmation was possible for untrusted projects.	8.8	More Details
CVE-2021-21870	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.4.37651. A specially crafted PDF document can trigger the reuse of previously free memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening a malicious file or site to trigger this vulnerability if the browser plugin extension is enabled.	8.8	More Details
CVE-2021-21893	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.0.0.49893. A specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2021-22517	A potential unauthorized privilege escalation vulnerability has been identified in Micro Focus Data Protector. The vulnerability affects versions 10.10, 10.20, 10.30, 10.40, 10.50, 10.60, 10.70, 10.80, 10.0 and 10.91. A privileged user may potentially misuse this feature and thus allow unintended and unauthorized access of data.	8.8	More Details
CVE-2021-24520	The Stock in & out WordPress plugin through 1.0.4 lacks proper sanitization before passing variables to an SQL request, making it vulnerable to SQL Injection attacks. Users with a role of contributor or higher can exploit this vulnerability.	8.8	More Details
CVE-2021-37381	Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private information such as photos through CSRF. For example: any student's photo information can be accessed through /gmis/(S([1]))/student/grgl/PotoImageShow/?bh=[2]. Among them, the code in [1] is a random string generated according to the user's login related information. It can protect the user's identity, but it can not effectively prevent unauthorized access. The code in [2] is the student number of any student. The attacker can carry out CSRF attack on the system by modifying [2] without modifying [1].	8.8	More Details
CVE-2021-37366	CTparental before 4.45.03 is vulnerable to cross-site request forgery (CSRF) in the CTparental admin panel. By combining CSRF with XSS, an attacker can trick the administrator into clicking a link that cancels the filtering for all standard users.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34633	The Youtube Feeder WordPress plugin is vulnerable to Cross-Site Request Forgery via the printAdminPage function found in the ~/youtube-feeder.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.1.	8.8	More Details
CVE-2021-34631	The NewsPlugin WordPress plugin is vulnerable to Cross-Site Request Forgery via the handle_save_style function found in the ~/news-plugin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.18.	8.8	More Details
CVE-2021-33708	Due to insufficient input validation in Kyma, authenticated users can pass a Header of their choice and escalate privileges.	8.8	More Details
CVE-2021-36483	DevExpress.XtraReports.UI through v21.1 allows attackers to execute arbitrary code via insecure deserialization.	8.8	More Details
CVE-2021-29970	A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. *This bug could only be triggered when accessibility was enabled.*. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90.	8.8	More Details
CVE-2021-38169	Roxy-WI through 5.2.2.0 allows command injection via /app/funct.py and /api/api_funct.py.	8.8	More Details
CVE-2021-38168	Roxy-WI through 5.2.2.0 allows authenticated SQL injection via select_servers.	8.8	More Details
CVE-2021-29972	A use-after-free vulnerability was found via testing, and traced to an out-of-date Cairo library. Updating the library resolved the issue, and may have remediated other, unknown security vulnerabilities as well. This vulnerability affects Firefox < 90.	8.8	More Details
CVE-2020-21688	A heap-use-after-free in the av_freep function in libavutil/mem.c of FFmpeg 4.2 allows attackers to execute arbitrary code.	8.8	More Details
CVE-2021-36276	Dell DBUtilDrv2.sys driver (versions 2.5 and 2.6) contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29973	Password autofill was enabled without user interaction on insecure websites on Firefox for Android. This was corrected to require user interaction with the page before a user's password would be entered by the browser's autofill functionality *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 90.	8.8	More Details
CVE-2021-29976	Mozilla developers reported memory safety bugs present in code shared between Firefox and Thunderbird. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90.	8.8	More Details
CVE-2021-29977	Mozilla developers reported memory safety bugs present in Firefox 89. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 90.	8.8	More Details
CVE-2021-32603	A server-side request forgery (SSRF) (CWE-918) vulnerability in FortiManager and FortiAnalyser GUI 7.0.0, 6.4.5 and below, 6.2.7 and below, 6.0.11 and below, 5.6.11 and below may allow a remote and authenticated attacker to access unauthorized files and services on the system via specifically crafted web requests.	8.8	More Details
CVE-2020-18694	Cross Site Request Forgery (CSRF) in IgnitedCMS v1.0 allows remote attackers to obtain sensitive information and gain privilege via the component "/admin/profile/save_profile".	8.8	More Details
CVE-2021-36800	Akaunting version 2.1.12 and earlier suffers from a code injection issue in the Money.php component of the application. A POST sent to /{company_id}/sales/invoices/{invoice_id} with an items[0][price] that includes a PHP callable function is executed directly. This issue was fixed in version 2.1.13 of the product.	8.7	More Details
CVE-2021-22241	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.0. It was possible to exploit a stored cross-site-scripting via a specifically crafted default branch name.	8.7	More Details
CVE-2021-3682	A flaw was found in the USB redirector device emulation of QEMU in versions prior to 6.1.0-rc2. It occurs when dropping packets during a bulk transfer from a SPICE client due to the packet queue being full. A malicious SPICE client could use this flaw to make QEMU call free() with faked heap chunk metadata, resulting in a crash of QEMU or potential code execution with the privileges of the QEMU process on the host.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1602	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the vulnerability, only commands without parameters can be executed.	8.2	More Details
CVE-2021-38290	A host header attack vulnerability exists in FUEL CMS 1.5.0 through fuel/modules/fuel/config/fuel_constants.php and fuel/modules/fuel/libraries/Asset.php. An attacker can use a man in the middle attack such as phishing.	8.1	More Details
CVE-2020-36436	An issue was discovered in the unicycle crate before 0.7.1 for Rust. PinSlab<T> and Unordered<T, S> do not have bounds on their Send and Sync traits.	8.1	More Details
CVE-2021-32581	Acronis True Image prior to 2021 Update 4 for Windows, Acronis True Image prior to 2021 Update 5 for Mac, Acronis Agent prior to build 26653, Acronis Cyber Protect prior to build 27009 did not implement SSL certificate validation.	8.1	More Details
CVE-2021-36801	Akaunting version 2.1.12 and earlier suffers from an authentication bypass issue in the user-controllable field, companies[0]. This issue was fixed in version 2.1.13 of the product.	8.1	More Details
CVE-2021-24501	The Workreap WordPress theme before 2.2.2 had several AJAX actions missing authorization checks to verify that a user was authorized to perform critical operations such as modifying or deleting objects. This allowed a logged in user to modify or delete objects belonging to other users on the site.	8.1	More Details
CVE-2021-24500	Several AJAX actions available in the Workreap WordPress theme before 2.2.2 lacked CSRF protections, as well as allowing insecure direct object references that were not validated. This allows an attacker to trick a logged in user to submit a POST request to the vulnerable site, potentially modifying or deleting arbitrary objects on the target site.	8.1	More Details
CVE-2021-22927	A session fixation vulnerability exists in Citrix ADC and Citrix Gateway 13.0-82.45 when configured SAML service provider that could allow an attacker to hijack a session.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36435	An issue was discovered in the ruspiro-singleton crate before 0.4.1 for Rust. In Singleton, Send and Sync do not have bounds checks.	8.1	More Details
CVE-2020-36463	An issue was discovered in the multiqueue crate through 2020-12-25 for Rust. There are unconditional implementations of Send for InnerSend<RW, T>, InnerRecv<RW, T>, FutInnerSend<RW, T>, and FutInnerRecv<RW, T>.	8.1	More Details
CVE-2021-37632	SuperMartijn642's Config Lib is a library used by a number of mods for the game Minecraft. The versions of SuperMartijn642's Config Lib between 1.0.4 and 1.0.8 are affected by a vulnerability and can be exploited on both servers and clients. Using SuperMartijn642's Config Lib, servers will send a packet to clients with the server's config values. In order to read `enum` values from the packet data, `ObjectInputStream#readObject` is used. `ObjectInputStream#readObject` will instantiate a class based on the input data. Since, the packet data is not validated before `ObjectInputStream#readObject` is called, an attacker can instantiate any class by sending a malicious packet. If a suitable class is found, the vulnerability can lead to a number of exploits, including remote code execution. Although the vulnerable packet is typically only send from server to client, it can theoretically also be send from client to server. This means both clients and servers running SuperMartijn642's Config Lib between 1.0.4 and 1.0.8 are vulnerable. The vulnerability has been patched in SuperMartijn642's Config lib 1.0.9. Both, players and server owners, should update to 1.0.9 or higher.	8.1	More Details
CVE-2020-36450	An issue was discovered in the bunch crate through 2020-11-12 for Rust. There are unconditional implementations of Send and Sync for Bunch<T>.	8.1	More Details
CVE-2020-36437	An issue was discovered in the conqueue crate before 0.4.0 for Rust. There are unconditional implementations of Send and Sync for QueueSender<T>.	8.1	More Details
CVE-2020-36438	An issue was discovered in the tiny_future crate before 0.4.0 for Rust. Future<T> does not have bounds on its Send and Sync traits.	8.1	More Details
CVE-2020-36439	An issue was discovered in the ticketed_lock crate before 0.3.0 for Rust. There are unconditional implementations of Send for ReadTicket<T> and WriteTicket<T>.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36440	An issue was discovered in the libsbc crate before 0.1.5 for Rust. For Decoder<R>, it implements Send for any R: Read.	8.1	More Details
CVE-2020-36441	An issue was discovered in the abox crate before 0.4.1 for Rust. It implements Send and Sync for AtomicBox<T> with no requirement for T: Send and T: Sync.	8.1	More Details
CVE-2020-36442	An issue was discovered in the beef crate before 0.5.0 for Rust. beef::Cow has no Sync bound on its Send trait.	8.1	More Details
CVE-2020-36444	An issue was discovered in the async-coap crate through 2020-12-08 for Rust. Send and Sync are implemented for ArcGuard<RC, T> without trait bounds on RC.	8.1	More Details
CVE-2020-36445	An issue was discovered in the convec crate through 2020-11-24 for Rust. There are unconditional implementations of Send and Sync for ConVec<T>.	8.1	More Details
CVE-2021-24010	Improper limitation of a pathname to a restricted directory vulnerabilities in FortiSandbox 3.2.0 through 3.2.2, and 3.1.0 through 3.1.4 may allow an authenticated user to obtain unauthorized access to files and data via specifially crafted web requests.	8.1	More Details
CVE-2020-36446	An issue was discovered in the signal-simple crate through 2020-11-15 for Rust. There are unconditional implementations of Send and Sync for SyncChannel<T>.	8.1	More Details
CVE-2020-36447	An issue was discovered in the v9 crate through 2020-12-18 for Rust. There is an unconditional implementation of Sync for SyncRef<T>.	8.1	More Details
CVE-2020-36448	An issue was discovered in the cache crate through 2020-11-24 for Rust. There are unconditional implementations of Send and Sync for Cache<K>.	8.1	More Details
CVE-2020-36449	An issue was discovered in the kekbit crate before 0.3.4 for Rust. For ShmWriter<H>, Send is implemented without requiring H: Send.	8.1	More Details
CVE-2021-38137	Corero SecureWatch Managed Services 9.7.2.0020 does not correctly check swa-monitor and cns-monitor user’s privileges, allowing a user to perform actions not belonging to his role.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36451	An issue was discovered in the rcu_cell crate through 2020-11-14 for Rust. There are unconditional implementations of Send and Sync for RcuCell<T>.	8.1	More Details
CVE-2020-36457	An issue was discovered in the lever crate before 0.1.1 for Rust. AtomicBox<T> implements the Send and Sync traits for all types T.	8.1	More Details
CVE-2020-36461	An issue was discovered in the noise_search crate through 2020-12-10 for Rust. There are unconditional implementations of Send and Sync for MvccRwLock.	8.1	More Details
CVE-2020-36460	An issue was discovered in the model crate through 2020-11-10 for Rust. The Shared data structure has an implementation of the Send and Sync traits without regard for the inner type.	8.1	More Details
CVE-2020-36453	An issue was discovered in the scottqueue crate through 2020-11-15 for Rust. There are unconditional implementations of Send and Sync for Queue<T>.	8.1	More Details
CVE-2020-36458	An issue was discovered in the lexer crate through 2020-11-10 for Rust. For ReaderResult<T, E>, there is an implementation of Sync with a trait bound of T: Send, E: Send.	8.1	More Details
CVE-2020-36459	An issue was discovered in the dces crate through 2020-12-09 for Rust. The World type is marked as Send but lacks bounds on its EntityStore and ComponentStore.	8.1	More Details
CVE-2020-36456	An issue was discovered in the toolshed crate through 2020-11-15 for Rust. In CopyCell<T>, the Send trait lacks bounds on the contained type.	8.1	More Details
CVE-2020-36455	An issue was discovered in the slock crate through 2020-11-17 for Rust. Slock<T> unconditionally implements Send and Sync.	8.1	More Details
CVE-2020-36454	An issue was discovered in the parc crate through 2020-11-14 for Rust. LockWeak<T> has an unconditional implementation of Send without trait bounds on T.	8.1	More Details
CVE-2020-36462	An issue was discovered in the syncpool crate before 0.1.6 for Rust. There is an unconditional implementation of Send for Bucket2.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32003	Unprotected Transport of Credentials vulnerability in SiteManager provisioning service allows local attacker to capture credentials if the service is used after provisioning. This issue affects: Secomea SiteManager All versions prior to 9.5 on Hardware.	8.0	More Details
CVE-2021-38305	23andMe Yamale before 3.0.8 allows remote attackers to execute arbitrary code via a crafted schema file. The schema parser uses eval as part of its processing, and tries to protect from malicious expressions by limiting the builtins that are passed to the eval. When processing the schema, each line is run through Python's eval function to make the validator available. A well-constructed string within the schema rules can execute system commands; thus, by exploiting the vulnerability, an attacker can run arbitrary code on the image that invokes Yamale.	7.8	More Details
CVE-2021-38160	In drivers/char/virtio_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size. NOTE: the vendor indicates that the cited data corruption is not a vulnerability in any existing use case; the length validation was added solely for robustness in the face of anomalous host OS behavior	7.8	More Details
CVE-2021-36277	Dell Command | Update, Dell Update, and Alienware Update versions before 4.3 contains an Improper Verification of Cryptographic Signature Vulnerability. A local authenticated malicious user may exploit this vulnerability by executing arbitrary code on the system.	7.8	More Details
CVE-2021-38185	GNU cpio through 2.13 allows attackers to execute arbitrary code via a crafted pattern file, because of a dstring.c ds_fgetstr integer overflow that triggers an out-of-bounds heap write. NOTE: it is unclear whether there are common cases where the pattern file, associated with the -E option, is untrusted data.	7.8	More Details
CVE-2021-38166	In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow and out-of-bounds write when many elements are placed in a single bucket. NOTE: exploitation might be impractical without the CAP_SYS_ADMIN capability.	7.8	More Details
CVE-2021-28216	BootPerformanceTable pointer is read from an NVRAM variable in PEI. Recommend setting PcdFirmwarePerformanceDataTableS3Support to FALSE.	7.8	More Details
CVE-2021-32578	Acronis True Image prior to 2021 Update 4 for Windows allowed local privilege escalation due to improper soft link handling (issue 2 of 2).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22928	A vulnerability has been identified in Citrix Virtual Apps and Desktops that could, if exploited, allow a user of a Windows VDA that has either Citrix Profile Management or Citrix Profile Management WMI Plugin installed to escalate their privilege level on that Windows VDA to SYSTEM.	7.8	More Details
CVE-2021-32577	Acronis True Image prior to 2021 Update 5 for Windows allowed local privilege escalation due to insecure folder permissions.	7.8	More Details
CVE-2021-32579	Acronis True Image prior to 2021 Update 4 for Windows and Acronis True Image prior to 2021 Update 5 for macOS allowed an unauthenticated attacker (who has a local code execution ability) to tamper with the micro-service API.	7.8	More Details
CVE-2021-32580	Acronis True Image prior to 2021 Update 4 for Windows allowed local privilege escalation due to DLL hijacking.	7.8	More Details
CVE-2021-35312	A vulnerability was found in CIR 2000 / Gestionale Amica Prodigy v1.7. The Amica Prodigy's executable "RemoteBackup.Service.exe" has incorrect permissions, allowing a local unprivileged user to replace it with a malicious file that will be executed with "LocalSystem" privileges.	7.8	More Details
CVE-2021-36795	A permission issue in the Cohesity Linux agent may allow privilege escalation in version 6.5.1b to 6.5.1d-hotfix10, 6.6.0a to 6.6.0b-hotfix1. An underprivileged linux user, if certain environment criteria are met, can gain additional privileges.	7.8	More Details
CVE-2020-24742	An issue has been fixed in Qt versions 5.14.0 where QPluginLoader attempts to load plugins relative to the working directory, allowing attackers to execute arbitrary code via crafted files.	7.8	More Details
CVE-2021-32576	Acronis True Image prior to 2021 Update 4 for Windows allowed local privilege escalation due to improper soft link handling (issue 1 of 2).	7.8	More Details
CVE-2021-34833	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14023.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21567	Dell PowerScale OneFS 9.1.0.x contains an improper privilege management vulnerability. It may allow an authenticated user with ISI_PRIV_LOGIN_SSH and/or ISI_PRIV_LOGIN_CONSOLE to elevate privilege.	7.8	More Details
CVE-2021-34842	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14024.	7.8	More Details
CVE-2021-34841	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14022.	7.8	More Details
CVE-2021-1572	A vulnerability in ConfD could allow an authenticated, local attacker to execute arbitrary commands at the level of the account under which ConfD is running, which is commonly root. To exploit this vulnerability, an attacker must have a valid account on an affected device. The vulnerability exists because the affected software incorrectly runs the SFTP user service at the privilege level of the account that was running when the ConfD built-in Secure Shell (SSH) server for CLI was enabled. If the ConfD built-in SSH server was not enabled, the device is not affected by this vulnerability. An attacker with low-level privileges could exploit this vulnerability by authenticating to an affected device and issuing a series of commands at the SFTP interface. A successful exploit could allow the attacker to elevate privileges to the level of the account under which ConfD is running, which is commonly root. Note: Any user who can authenticate to the built-in SSH server may exploit this vulnerability. By default, all ConfD users have this access if the server is enabled. Software updates that address this vulnerability have been released.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34840	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14021.	7.8	More Details
CVE-2021-34839	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14020.	7.8	More Details
CVE-2021-37367	CTparental before 4.45.07 is affected by a code execution vulnerability in the CTparental admin panel. Because The file "bl_categories_help.php" is vulnerable to directory traversal, an attacker can create a file that contains scripts and run arbitrary commands.	7.8	More Details
CVE-2021-34831	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.4.37651. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Document objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13741.	7.8	More Details
CVE-2021-22385	A component of the Huawei smartphone has a External Control of System or Configuration Setting vulnerability. Local attackers may exploit this vulnerability to cause Kernel Code Execution.	7.8	More Details
CVE-2021-34832	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the delay property. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13928.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34838	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14019.	7.8	More Details
CVE-2021-34848	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14532.	7.8	More Details
CVE-2021-34834	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14014.	7.8	More Details
CVE-2021-34837	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14018.	7.8	More Details
CVE-2021-34835	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14015.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34836	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14017.	7.8	More Details
CVE-2021-34843	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14025.	7.8	More Details
CVE-2021-34844	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14033.	7.8	More Details
CVE-2021-37179	A vulnerability has been identified in Solid Edge SE2021 (All Versions < SE2021MP7). The PSKERNEL.dll library in affected application lacks proper validation while parsing user-supplied OBJ files that could lead to a use-after-free condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13777)	7.8	More Details
CVE-2021-21863	A unsafe deserialization vulnerability exists in the ComponentModel Profile.FromFile() functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34849	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14531.	7.8	More Details
CVE-2021-34850	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14529.	7.8	More Details
CVE-2021-34851	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14016.	7.8	More Details
CVE-2021-37180	A vulnerability has been identified in Solid Edge SE2021 (All Versions < SE2021MP7). The PSKERNEL.dll library lacks proper validation while parsing user-supplied OBJ files that could cause an out of bounds access to an uninitialized pointer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13775)	7.8	More Details
CVE-2021-34847	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14270.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34852	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13929.	7.8	More Details
CVE-2021-34846	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14120.	7.8	More Details
CVE-2021-34845	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14034.	7.8	More Details
CVE-2021-34853	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14013.	7.8	More Details
CVE-2021-32464	An incorrect permission assignment privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security Services could allow an attacker to modify a specific script before it is executed. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21584	Dell OpenManage Enterprise version 3.5 and OpenManage Enterprise-Modular version 1.30.00 contain an information disclosure vulnerability. An authenticated low privileged attacker may potentially exploit this vulnerability leading to disclosure of the OIDC server credentials.	7.7	More Details
CVE-2021-32706	Pi-hole's Web interface provides a central location to manage a Pi-hole instance and review performance statistics. Prior to Pi-hole Web interface version 5.5.1, the `validDomainWildcard` preg_match filter allows a malicious character through that can be used to execute code, list directories, and overwrite sensitive files. The issue lies in the fact that one of the periods is not escaped, allowing any character to be used in its place. A patch for this vulnerability was released in version 5.5.1.	7.6	More Details
CVE-2021-36708	In ProLink PRC2402M V1.0.18 and older, the set_sys_init function in the login.cgi binary allows an attacker to reset the password to the administrative interface of the router.	7.5	More Details
CVE-2020-36464	An issue was discovered in the heapless crate before 0.6.1 for Rust. The IntoIter Clone implementation clones an entire underlying Vec without considering whether it has already been partially consumed.	7.5	More Details
CVE-2020-36465	An issue was discovered in the generic-array crate before 0.13.3 for Rust. It violates soundness by using the arr! macro to extend lifetimes.	7.5	More Details
CVE-2021-38192	An issue was discovered in the prost-types crate before 0.8.0 for Rust. An overflow can occur during conversion from Timestamp to SystemTime.	7.5	More Details
CVE-2021-37545	In JetBrains TeamCity before 2021.1.1, insufficient authentication checks for agent requests were made.	7.5	More Details
CVE-2021-3580	A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use this flaw to provide a manipulated ciphertext leading to application crash and denial of service.	7.5	More Details
CVE-2021-21501	Improper configuration will cause ServiceComb ServiceCenter Directory Traversal problem in ServcieCenter 1.x.x versions and fixed in 2.0.0.	7.5	More Details
CVE-2021-37548	In JetBrains TeamCity before 2021.1, passwords in cleartext sometimes could be stored in VCS.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37550	In JetBrains YouTrack before 2021.2.16363, time-unsafe comparisons were used.	7.5	More Details
CVE-2020-36433	An issue was discovered in the chunky crate through 2020-08-25 for Rust. The Chunk API does not honor an alignment requirement.	7.5	More Details
CVE-2021-38511	An issue was discovered in the tar crate before 0.4.36 for Rust. When symlinks are present in a TAR archive, extraction can create arbitrary directories via .. traversal.	7.5	More Details
CVE-2021-38490	Altova MobileTogether Server before 7.3 SP1 allows XML exponential entity expansion, a different vulnerability than CVE-2021-37425.	7.5	More Details
CVE-2021-29765	IBM PowerVM Hypervisor FW940 and FW950 could allow an attacker to obtain sensitive information if they gain service access to the FSP. IBM X-Force ID: 202476.	7.5	More Details
CVE-2021-29923	Go before 1.17 does not properly consider extraneous zero characters at the beginning of an IP address octet, which (in some situations) allows attackers to bypass access control that is based on IP addresses, because of unexpected octal interpretation. This affects net.ParseIP and net.ParseCIDR.	7.5	More Details
CVE-2020-28087	A SQL injection vulnerability in /jeecg boot/sys/dict/loadtreedata of jeecg-boot CMS 2.3 allows attackers to access sensitive database information.	7.5	More Details
CVE-2021-35397	A path traversal vulnerability in the static router for Drogon from 1.0.0-beta14 to 1.6.0 could allow an unauthenticated, remote attacker to arbitrarily read files. The vulnerability is due to lack of proper input validation for requested path. An attacker could exploit this vulnerability by sending crafted HTTP request with specific path to read. Successful exploitation could allow the attacker to read files that should be restricted.	7.5	More Details
CVE-2021-33338	The Layout module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 6, exposes the CSRF token in URLs, which allows man-in-the-middle attackers to obtain the token and conduct Cross-Site Request Forgery (CSRF) attacks via the p_auth parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29296	Null Pointer Dereference vulnerability in D-Link DIR-825 2.10b02, which could let a remote malicious user cause a denial of service. The vulnerability could be triggered by sending an HTTP request with URL /vct_wan; the sbin/httpd would invoke the strchr function and take NULL as a first argument, which finally leads to the segmentation fault. NOTE: The DIR-825 and all hardware revisions is considered End of Life and as such this issue will not be patched	7.5	More Details
CVE-2021-36764	In CODESYS Gateway V3 before 3.5.17.10, there is a NULL Pointer Dereference. Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and may result in a denial-of-service condition.	7.5	More Details
CVE-2021-36765	In CODESYS EtherNetIP before 4.1.0.0, specific EtherNet/IP requests may cause a null pointer dereference in the downloaded vulnerable EtherNet/IP stack that is executed by the CODESYS Control runtime system.	7.5	More Details
CVE-2021-38155	OpenStack Keystone 10.x through 16.x before 16.0.2, 17.x before 17.0.1, 18.x before 18.0.1, and 19.x before 19.0.1 allows information disclosure during account locking (related to PCI DSS features). By guessing the name of an account and failing to authenticate multiple times, any unauthenticated actor could both confirm the account exists and obtain that account's corresponding UUID, which might be leveraged for other unrelated attacks. All deployments enabling security_compliance.lockout_failure_attempts are affected.	7.5	More Details
CVE-2021-29295	Null Pointer Dereference vulnerability exists in D-Link DSP-W215 1.10, which could let a remote malicious user cause a denial of servie via usr/bin/lighttpd. It could be triggered by sending an HTTP request without URL in the start line directly to the device. NOTE: The DSP-W215 and all hardware revisions is considered End of Life and as such this issue will not be patched	7.5	More Details
CVE-2021-29294	Null Pointer Dereference vulnerability exists in D-Link DSL-2740R UK_1.01, which could let a remove malicious user cause a denial of service via the send_hnap_unauthorized function. It could be triggered by sending crafted POST request to /HNAP1/. NOTE: The DSL-2740R and all hardware revisions are considered End of Life and as such this issue will not be patched	7.5	More Details
CVE-2021-28845	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38387	In Contiki 3.0, a Telnet server that silently quits (before disconnection with clients) leads to connected clients entering an infinite loop and waiting forever, which may cause excessive CPU consumption.	7.5	More Details
CVE-2021-20594	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Mitsubishi Electric MELSEC iQ-R series Safety CPU modules R08/16/32/120SFCPU firmware versions "26" and prior and Mitsubishi Electric MELSEC iQ-R series SIL2 Process CPU modules R08/16/32/120PSFCPU firmware versions "11" and prior allows a remote unauthenticated attacker to acquire legitimate user names registered in the module via brute-force attack on user names.	7.5	More Details
CVE-2021-38386	In Contiki 3.0, a buffer overflow in the Telnet service allows remote attackers to cause a denial of service because the ls command is mishandled when a directory has many files with long names.	7.5	More Details
CVE-2021-28844	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03 by sending the POST request to apply_cgi via a do_graph_auth action without a session_id key.	7.5	More Details
CVE-2021-28843	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03 by sending the POST request to apply_cgi with an unknown action name.	7.5	More Details
CVE-2021-28842	Null Pointer Deference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial os service by sending the POST request to apply_cgi via action do_graph_auth without login_name key.	7.5	More Details
CVE-2021-28841	Null Pointer Dereference vulnerability in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending a POST request to apply_cgi via an action ping_test without a ping_ipaddr key.	7.5	More Details
CVE-2021-37553	In JetBrains YouTrack before 2021.2.16363, an insecure PRNG was used.	7.5	More Details
CVE-2021-38201	net/sunrpc/xdr.c in the Linux kernel before 5.13.4 allows remote attackers to cause a denial of service (xdr_set_page_base slab-out-of-bounds access) by performing many NFS 4.2 READ_PLUS operations.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38202	fs/nfsd/trace.h in the Linux kernel before 5.13.4 might allow remote attackers to cause a denial of service (out-of-bounds read in strlen) by sending NFS traffic when the trace event framework is being used for nfsd.	7.5	More Details
CVE-2021-37156	Redmine 4.2.0 and 4.2.1 allow existing user sessions to continue upon enabling two-factor authentication for the user's account, but the intended behavior is for those sessions to be terminated.	7.5	More Details
CVE-2021-38095	The REST API in Planview Spigit 4.5.3 allows remote unauthenticated attackers to query sensitive user accounts data, as demonstrated by an api/v1/users/1 request.	7.5	More Details
CVE-2021-1630	XML external entity (XXE) vulnerability affecting certain versions of a Mule runtime component that may affect CloudHub, GovCloud, Runtime Fabric, Pivotal Cloud Foundry, Private Cloud Edition, and on-premise customers.	7.5	More Details
CVE-2021-28840	Null Pointer Dereference vulnerability exists in D-Link DAP-2310 2.07.RC031, DAP-2330 1.07.RC028, DAP-2360 2.07.RC043, DAP-2553 3.06.RC027, DAP-2660 1.13.RC074, DAP-2690 3.16.RC100, DAP-2695 1.17.RC063, DAP-3320 1.01.RC014 and DAP-3662 1.01.RC022 in the upload_config function of sbin/httpd binary. When the binary handle the specific HTTP GET request, the content in upload_file variable is NULL in the upload_config function then the strncasecmp would take NULL as first argument, and incur the NULL pointer dereference vulnerability.	7.5	More Details
CVE-2021-28839	Null Pointer Dereference vulnerability exists in D-Link DAP-2310 2.07.RC031, DAP-2330 1.07.RC028, DAP-2360 2.07.RC043, DAP-2553 3.06.RC027, DAP-2660 1.13.RC074, DAP-2690 3.16.RC100, DAP-2695 1.17.RC063, DAP-3320 1.01.RC014 and DAP-3662 1.01.RC022 in the upload_certificate function of sbin/httpd binary. When the binary handle the specific HTTP GET request, the strrchr in the upload_certificate function would take NULL as first argument, and incur the NULL pointer dereference vulnerability.	7.5	More Details
CVE-2021-35326	A vulnerability in TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows attackers to download the configuration file via sending a crafted HTTP request.	7.5	More Details
CVE-2015-2073	The File RepositoRy Server (FRS) CORBA listener in SAP BussinessObjects Edge 4.0 allows remote attackers to read arbitrary files via a full pathname, aka SAP Note 2018682.	7.5	More Details
CVE-2015-2074	The File Repository Server (FRS) CORBA listener in SAP BussinessObjects Edge 4.0 allows remote attackers to write to arbitrary files via a full pathname, aka SAP Note 2018681.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38371	The STARTTLS feature in Exim through 4.94.2 allows response injection (buffering) during MTA SMTP sending.	7.5	More Details
CVE-2021-3689	yii2 is vulnerable to Use of Predictable Algorithm in Random Number Generator	7.5	More Details
CVE-2021-37604	In version 6.5 of Microchip MiWi software and all previous versions including legacy products, there is a possibility of frame counters being validated/updated prior to the message authentication. With this vulnerability in place, an attacker may increment the incoming frame counter values by injecting messages with a sufficiently large frame counter value and invalid payload. This results in denial of service/valid packets in the network. There is also a possibility of a replay attack in the stack.	7.5	More Details
CVE-2021-20592	Missing synchronization vulnerability in GOT2000 series GT27 model communication driver versions 01.19.000 through 01.39.010, GT25 model communication driver versions 01.19.000 through 01.39.010 and GT23 model communication driver versions 01.19.000 through 01.39.010 and GT SoftGOT2000 versions 1.170C through 1.256S allows a remote unauthenticated attacker to cause DoS condition on the MODBUS/TCP slave communication function of the products by rapidly and repeatedly connecting and disconnecting to and from the MODBUS/TCP communication port on a target. Restart or reset is required to recover.	7.5	More Details
CVE-2021-37605	In version 6.5 Microchip MiWi software and all previous versions including legacy products, the stack is validating only two out of four Message Integrity Check (MIC) bytes.	7.5	More Details
CVE-2021-37172	A vulnerability has been identified in SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (V4.5.0). Affected devices fail to authenticate against configured passwords when provisioned using TIA Portal V13. This could allow an attacker using TIA Portal V13 or later versions to bypass authentication and download arbitrary programs to the PLC. The vulnerability does not occur when TIA Portal V13 SP1 or any later version was used to provision the device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37625	Skytable is an open source NoSQL database. In versions prior to 0.6.4 an incorrect check of return value of the accept function in the run-loop for a TCP socket/TLS socket/TCP+TLS multi-socket causes an early exit from the run loop that should continue infinitely unless terminated by a local user, effectively causing the whole database server to shut down. This has severe impact and can be used to easily cause DoS attacks without the need to use much bandwidth. The attack vectors include using an incomplete TLS connection for example by not providing the certificate for the connection and using a specially crafted TCP packet that triggers the application layer backoff algorithm.	7.5	More Details
CVE-2021-25659	A vulnerability has been identified in Automation License Manager 5 (All versions), Automation License Manager 6 (All versions < V6.0 SP9 Update 2). Sending specially crafted packets to port 4410/tcp of an affected system could lead to extensive memory being consumed and as such could cause a denial-of-service preventing legitimate users from using the system.	7.5	More Details
CVE-2021-38311	In Contiki 3.0, potential nonterminating acknowledgment loops exist in the Telnet service. When the negotiated options are already disabled, servers still respond to DONT and WONT requests with WONT or DONT commands, which may lead to infinite acknowledgment loops, denial of service, and excessive CPU consumption.	7.5	More Details
CVE-2020-23148	The userLogin parameter in ldap/login.php of rConfig 3.9.5 is unsanitized, allowing attackers to perform a LDAP injection and obtain sensitive information via a crafted POST request.	7.5	More Details
CVE-2020-23149	The dbName parameter in ajaxDbInstall.php of rConfig 3.9.5 is unsanitized, allowing attackers to perform a SQL injection and access sensitive database information.	7.5	More Details
CVE-2020-23150	A SQL injection vulnerability in config.inc.php of rConfig 3.9.5 allows attackers to access sensitive database information via a crafted GET request to install/lib/ajaxHandlers/ajaxDbInstall.php.	7.5	More Details
CVE-2021-38380	Live555 through 1.08 mishandles huge requests for the same MP3 stream, leading to recursion and s stack-based buffer over-read. An attacker can leverage this to launch a DoS attack.	7.5	More Details
CVE-2021-28838	Null pointer dereference vulnerability in D-Link DAP-2310 2,10RC039, DAP-2330 1.10RC036 BETA, DAP-2360 2.10RC055, DAP-2553 3.10rc039 BETA, DAP-2660 1.15rc131b, DAP-2690 3.20RC115 BETA, DAP-2695 1.20RC093, DAP-3320 1.05RC027 BETA and DAP-3662 1.05rc069 in the sbin/httpd binary. The crash happens at the `atoi' operation when a specific network package are sent to the httpd binary.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36798	A Denial-of-Service (DoS) vulnerability was discovered in Team Server in HelpSystems Cobalt Strike 4.2 and 4.3. It allows remote attackers to crash the C2 server thread and block beacons' communication with it.	7.5	More Details
CVE-2021-22926	libcurl-using applications can ask for a specific client certificate to be used in a transfer. This is done with the `CURLOPT_SSLCERT` option (`--cert` with the command line tool).When libcurl is built to use the macOS native TLS library Secure Transport, an application can ask for the client certificate by name or with a file name - using the same option. If the name exists as a file, it will be used instead of by name.If the appliction runs with a current working directory that is writable by other users (like `/tmp`), a malicious user can create a file name with the same name as the app wants to use by name, and thereby trick the application to use the file based cert instead of the one referred to by name making libcurl send the wrong client certificate in the TLS connection handshake.	7.5	More Details
CVE-2021-35325	A stack overflow in the checkLoginUser function of TOTOLINK A720R A720R_Firmware v4.1.5cu.470_B20200911 allows attackers to cause a denial of service (DOS).	7.5	More Details
CVE-2021-34639	Authenticated File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png" which is executable in some configurations. This issue affects: WordPress Download Manager version 3.1.24 and prior versions.	7.5	More Details
CVE-2021-23849	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera.	7.5	More Details
CVE-2021-26605	An improper input validation vulnerability in the service of ezPDFReader allows attacker to execute arbitrary command. This issue occurred when the ezPDF launcher received and executed crafted input values through JSON-RPC communication.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26586	A potential security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software. The vulnerability could be remotely exploited to disclose sensitive information. HPE has made software updates available to resolve the vulnerability in the HPE Edgeline Infrastructure Manager (EIM).	7.5	More Details
CVE-2021-38207	drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer overflow and lockup) by sending heavy network traffic for about ten minutes.	7.5	More Details
CVE-2021-22919	A vulnerability has been discovered in Citrix ADC (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway), and Citrix SD-WAN WANOP Edition models 4000-WO, 4100-WO, 5000-WO, and 5100-WO. These vulnerabilities, if exploited, could lead to the limited available disk space on the appliances being fully consumed.	7.5	More Details
CVE-2021-22124	An uncontrolled resource consumption (denial of service) vulnerability in the login modules of FortiSandbox 3.2.0 through 3.2.2, 3.1.0 through 3.1.4, and 3.0.0 through 3.0.6; and FortiAuthenticator before 6.0.6 may allow an unauthenticated attacker to bring the device into an unresponsive state via specifically-crafted long request parameters.	7.5	More Details
CVE-2021-38512	An issue was discovered in the actix-http crate before 3.0.0-beta.9 for Rust. HTTP/1 request smuggling (aka HRS) can occur, potentially leading to credential disclosure.	7.5	More Details
CVE-2021-37633	Discourse is an open source discussion platform. In versions prior to 2.7.8 rendering of d-popover tooltips can be susceptible to XSS attacks. This vulnerability only affects sites which have modified or disabled Discourse's default Content Security Policy. This issue is patched in the latest `stable` 2.7.8 version of Discourse. As a workaround users may ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.	7.4	More Details
CVE-2021-32797	JupyterLab is a user interface for Project Jupyter which will eventually replace the classic Jupyter Notebook. In affected versions untrusted notebook can execute code on load. In particular JupyterLab doesn’t sanitize the action attribute of html `<form>`. Using this it is possible to trigger the form validation outside of the form itself. This is a remote code execution, but requires user action to open a notebook.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37634	Leafkit is a templating language with Swift-inspired syntax. Versions prior to 1.3.0 are susceptible to Cross-site Scripting (XSS) attacks. This affects anyone passing unsanitised data to Leaf's variable tags. Before this fix, Leaf would not escape any strings passed to tags as variables. If an attacker managed to find a variable that was rendered with their unsanitised data, they could inject scripts into a generated Leaf page, which could enable XSS attacks if other mitigations such as a Content Security Policy were not enabled. This has been patched in 1.3.0. As a workaround sanitize any untrusted input before passing it to Leaf and enable a CSP to block inline script and CSS data.	7.4	More Details
CVE-2021-23419	This affects the package open-graph before 0.2.6. The function parse could be tricked into adding or modifying properties of Object.prototype using a __proto__ or constructor payload.	7.3	More Details
CVE-2021-1593	A vulnerability in Cisco Packet Tracer for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path on the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow an attacker with normal user privileges to execute arbitrary code on the affected system with the privileges of another user’s account.	7.3	More Details
CVE-2021-21597	Dell Wyse ThinOS, version 9.0, contains a Sensitive Information Disclosure Vulnerability. An authenticated malicious user with physical access to the system could exploit this vulnerability to read sensitive information written to the log files.	7.2	More Details
CVE-2021-33721	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2). The affected application incorrectly neutralizes special elements when creating batch operations which could lead to command injection. An authenticated remote attacker with administrative privileges could exploit this vulnerability to execute arbitrary code on the system with system privileges.	7.2	More Details
CVE-2021-24521	The Side Menu Lite – add sticky fixed buttons WordPress plugin before 2.2.1 does not properly sanitize input values from the browser when building an SQL statement. Users with the administrator role or permission to manage this plugin could perform an SQL Injection attack.	7.2	More Details
CVE-2021-37859	Fixed a bypass for a reflected cross-site scripting vulnerability affecting OAuth-enabled instances of Mattermost.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22386	A component of the Huawei smartphone has a Double Free vulnerability. Local attackers may exploit this vulnerability to cause Root Elevation of Privileges.	7.0	More Details
CVE-2021-38204	drivers/usb/host/max3421-hcd.c in the Linux kernel before 5.13.6 allows physically proximate attackers to cause a denial of service (use-after-free and panic) by removing a MAX-3421 USB device in certain situations.	6.8	More Details
CVE-2021-38199	fs/nfs/nfs4client.c in the Linux kernel before 5.13.4 has incorrect connection-setup ordering, which allows operators of remote NFSv4 servers to cause a denial of service (hanging of mounts) by arranging for those servers to be unreachable during trunking detection.	6.5	More Details
CVE-2021-29400	A cross-site request forgery (CSRF) vulnerability in the My SMTP Contact v1.1.1 plugin for GetSimple CMS allows remote attackers to change the SMTP settings of the contact forms for the webpages of the CMS after an authenticated admin visits a malicious third-party site.	6.5	More Details
CVE-2021-29714	IBM Content Navigator 3.0.CD could allow a malicious user to cause a denial of service due to improper input validation. IBM X-Force ID: 200968.	6.5	More Details
CVE-2020-21697	A heap-use-after-free in the mpeg_mux_write_packet function in libavformat/mpegenc.c of FFmpeg 4.2 allows to cause a denial of service (DOS) via a crafted avi file.	6.5	More Details
CVE-2021-24467	The Leaflet Map WordPress plugin before 3.0.0 does not verify the CSRF nonce when saving its settings, which allows attackers to make a logged in admin update the settings via a Cross-Site Request Forgery attack. This could lead to Cross-Site Scripting issues by either changing the URL of the JavaScript library being used, or using malicious attributions which will be executed in all page with an embed map from the plugin	6.5	More Details
CVE-2020-21677	A heap-based buffer overflow in the sixel_encoder_output_without_macro function in encoder.c of Libsixel 1.8.4 allows attackers to cause a denial of service (DOS) via converting a crafted PNG file into Sixel format.	6.5	More Details
CVE-2021-21600	Dell EMC NetWorker, 19.4 or older, contain an uncontrolled resource consumption flaw in its API service. An authorized API user could potentially exploit this vulnerability via the web and desktop user interfaces, leading to denial of service in the manageability path.	6.5	More Details
CVE-2021-38381	Live555 through 1.08 does not handle MPEG-1 or 2 files properly. Sending two successive RTSP SETUP commands for the same track causes a Use-After-Free and daemon crash.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28846	A Format String vulnerablity exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service due to a logic bug at address 0x40dcd0 when calling fprintf with "%s: key len = %d, too long\n" format. The two variables seem to be put in the wrong order. The vulnerability could be triggered by sending the POST request to apply_cgi with a long and unknown key in the request body.	6.5	More Details
CVE-2021-22674	The affected product is vulnerable to a relative path traversal condition, which may allow an attacker access to unauthorized files and directories on the WebAccess/SCADA (WebAccess/SCADA versions prior to 8.4.5, WebAccess/SCADA versions prior to 9.0.1).	6.5	More Details
CVE-2021-33699	Task Hijacking is a vulnerability that affects the applications running on Android devices due to a misconfiguration in their AndroidManifest.xml with their Task Control features. This allows an unauthorized attacker or malware to takeover legitimate apps and to steal user's sensitive information.	6.5	More Details
CVE-2021-38382	Live555 through 1.08 does not handle Matroska and Ogg files properly. Sending two successive RTSP SETUP commands for the same track causes a Use-After-Free and daemon crash.	6.5	More Details
CVE-2020-21358	A cross site request forgery (CSRF) in Wage-CMS 1.5.x-dev allows attackers to arbitrarily add users.	6.5	More Details
CVE-2021-35307	An issue was discovered in Bento4 through v1.6.0-636. A NULL pointer dereference exists in the AP4_DescriptorFinder::Test component located in /Core/Ap4Descriptor.h. It allows an attacker to cause a denial of service (DOS).	6.5	More Details
CVE-2021-35306	An issue was discovered in Bento4 through v1.6.0-636. A NULL pointer dereference exists in the function AP4_StszAtom::WriteFields located in Ap4StszAtom.cpp. It allows an attacker to cause a denial of service (DOS).	6.5	More Details
CVE-2021-37540	In JetBrains Hub before 2021.1.13262, a potentially insufficient CSP for the Widget deployment feature was used.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36168	A Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in Fortinet FortiPortal 6.x before 6.0.5, FortiPortal 5.3.x before 5.3.6 and any FortiPortal before 6.2.5 allows authenticated attacker to disclosure information via crafted GET request with malicious parameter values.	6.5	More Details
CVE-2021-36802	Akaunting version 2.1.12 and earlier suffers from a denial-of-service issue that is triggered by setting a malformed 'locale' variable and sending it in an otherwise normal HTTP POST request. This issue was fixed in version 2.1.13 of the product.	6.5	More Details
CVE-2021-22920	A vulnerability has been discovered in Citrix ADC (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway), and Citrix SD-WAN WANOP Edition models 4000-WO, 4100-WO, 5000-WO, and 5100-WO. These vulnerabilities, if exploited, could lead to a phishing attack through a SAML authentication hijack to steal a valid user session.	6.5	More Details
CVE-2021-34707	A vulnerability in the REST API of Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to access sensitive data on an affected system. This vulnerability exists because the application does not sufficiently protect sensitive data when responding to an API request. An attacker could exploit the vulnerability by sending a specific API request to the affected application. A successful exploit could allow the attacker to obtain sensitive information about the application.	6.5	More Details
CVE-2021-38136	Corero SecureWatch Managed Services 9.7.2.0020 is affected by a Path Traversal vulnerability via the snap_file parameter in the /it-IT/splunkd/__raw/services/get_snapshot HTTP API endpoint. A ‘low privileged’ attacker can read any file on the target host.	6.5	More Details
CVE-2021-31869	Pimcore AdminBundle version 6.8.0 and earlier suffers from a SQL injection issue in the specificID variable used by the application. This issue was fixed in version 6.9.4 of the product.	6.5	More Details
CVE-2021-31867	Pimcore Customer Data Framework version 3.0.0 and earlier suffers from a Boolean-based blind SQL injection issue in the $id parameter of the SegmentAssignmentController.php component of the application. This issue was fixed in version 3.0.2 of the product.	6.5	More Details
CVE-2021-29975	Through a series of DOM manipulations, a message, over which the attacker had control of the text but not HTML or formatting, could be overlaid on top of another domain (with the new domain correctly shown in the address bar) resulting in possible user confusion. This vulnerability affects Firefox < 90.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38115	read_header_tga in gd_tga.c in the GD Graphics Library (aka LibGD) through 2.3.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file.	6.5	More Details
CVE-2021-22922	When curl is instructed to download content using the metalink feature, thecontents is verified against a hash provided in the metalink XML file.The metalink XML file points out to the client how to get the same contentfrom a set of different URLs, potentially hosted by different servers and theclient can then download the file from one or several of them. In a serial orparallel manner.If one of the servers hosting the contents has been breached and the contentsof the specific file on that server is replaced with a modified payload, curlshould detect this when the hash of the file mismatches after a completeddownload. It should remove the contents and instead try getting the contentsfrom another URL. This is not done, and instead such a hash mismatch is onlymentioned in text and the potentially malicious content is kept in the file ondisk.	6.5	More Details
CVE-2021-34638	Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks, by setting Download template to a file containing configuration information or an uploaded JavaScript with an image extension This issue affects: WordPress Download Manager version 3.1.24 and prior versions.	6.5	More Details
CVE-2021-26096	Multiple instances of heap-based buffer overflow in the command shell of FortiSandbox before 4.0.0 may allow an authenticated attacker to manipulate memory and alter its content by means of specifically crafted command line arguments.	6.4	More Details
CVE-2021-36803	Akaunting version 2.1.12 and earlier suffers from a persistent (type II) cross-site scripting (XSS) vulnerability in processing user-supplied avatar images. This issue was fixed in version 2.1.13 of the product.	6.3	More Details
CVE-2021-3539	EspoCRM 6.1.6 and prior suffers from a persistent (type II) cross-site scripting (XSS) vulnerability in processing user-supplied avatar images. This issue was fixed in version 6.1.7 of the product.	6.3	More Details
CVE-2021-37390	A Chamilo LMS 1.11.14 reflected XSS vulnerability exists in main/social/search.php=q URI (social network search feature).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-17861	A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Portal/EPP allows remote attackers to inject arbitrary web script via the wsdlLib parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2021-37573	A reflected cross-site scripting (XSS) vulnerability in the web server TTiny Java Web Server and Servlet Container (TJWS) <=1.115 allows an adversary to inject malicious code on the server's "404 Page not Found" error page	6.1	More Details
CVE-2021-36601	GetSimpleCMS 3.3.16 contains a cross-site Scripting (XSS) vulnerability, where Function TSL does not filter check settings.php Website URL: "siteURL" parameter.	6.1	More Details
CVE-2021-33337	Cross-site scripting (XSS) vulnerability in the Document Library module's add document menu in Liferay Portal 7.3.0 through 7.3.4, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_document_library_web_portlet_DLAdminPortlet_name parameter.	6.1	More Details
CVE-2020-21357	A stored cross site scripting (XSS) vulnerability in /admin.php?mod=user&act=addnew of PopojiCMS 1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the E-Mail field.	6.1	More Details
CVE-2021-37389	Chamilo 1.11.14 allows stored XSS via main/install/index.php and main/install/ajax.php through the port parameter.	6.1	More Details
CVE-2021-24304	The Newsmag WordPress theme before 5.0 does not sanitise the td_block_id parameter in its td_ajax_block AJAX action, leading to an unauthenticated Reflected Cross-site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-38186	An issue was discovered in the comrak crate before 0.10.1 for Rust. It mishandles & characters, leading to XSS via &# HTML entities.	6.1	More Details
CVE-2021-24495	The Marmoset Viewer WordPress plugin before 1.9.3 does not property sanitize, validate or escape the 'id' parameter before outputting back in the page, leading to a reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2021-35463	Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.4.0 allows remote attackers to inject arbitrary web script or HTML into the management toolbar search via the `keywords` parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34661	The WP Fusion Lite WordPress plugin is vulnerable to Cross-Site Request Forgery via the `show_logs_section` function found in the ~/includes/admin/logging/class-log-handler.php file which allows attackers to drop all logs for the plugin, in versions up to and including 3.37.18.	6.1	More Details
CVE-2021-34660	The WP Fusion Lite WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the startdate parameter found in the ~/includes/admin/logging/class-log-table-list.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.37.18.	6.1	More Details
CVE-2021-24522	The User Registration, User Profile, Login & Membership – ProfilePress (Formerly WP User Avatar) WordPress plugin before 3.1.11's widget for tabbed login/register was not properly escaped and could be used in an XSS attack which could lead to wp-admin access. Further, the plugin in several places assigned $_POST as $_GET which meant that in some cases this could be replicated with just $_GET parameters and no need for $_POST values.	6.1	More Details
CVE-2018-17862	A cross-site scripting (XSS) vulnerability in SAP J2EE Engine/7.01/Fiori allows remote attackers to inject arbitrary web script via the sys_jdbc parameter to /TestJDBC_Web/test2. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2021-38193	An issue was discovered in the ammonia crate before 3.1.0 for Rust. XSS can occur because the parsing differences for HTML, SVG, and MathML are mishandled, a similar issue to CVE-2020-26870.	6.1	More Details
CVE-2021-33707	SAP NetWeaver Knowledge Management allows remote attackers to redirect users to arbitrary websites and conduct phishing attacks via a URL stored in a component. This could enable the attacker to compromise the user's confidentiality and integrity.	6.1	More Details
CVE-2021-21738	ZTE's big video business platform has two reflective cross-site scripting (XSS) vulnerabilities. Due to insufficient input verification, the attacker could implement XSS attacks by tampering with the parameters, to affect the operations of valid users. This affects: <ZXIPTV><ZXIPTV-EAS_PV5.06.04.09>	6.1	More Details
CVE-2020-22330	Cross-Site Scripting (XSS) vulnerability in Subrion 4.2.1 via the title when adding a page.	6.1	More Details
CVE-2021-37541	In JetBrains Hub before 2021.1.13402, HTML injection in the password reset email was possible.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37365	CTparental before 4.45.03 is vulnerable to cross-site scripting (XSS) in the CTparental admin panel. In bl_categires_help.php, the 'categories' variable is assigned with the content of the query string param 'cat' without sanitization or encoding, enabling an attacker to inject malicious code into the output webpage.	6.1	More Details
CVE-2021-20116	A reflected cross-site scripting vulnerability exists in TCExam <= 14.8.4. The paths provided in the f, d, and dir parameters in tce_select_mediafile.php were not properly validated and could cause reflected XSS via the unsanitized output of the path supplied. An attacker could craft a malicious link which, if triggered by an administrator, could result in the attacker hijacking the victim's session or performing actions on their behalf.	6.1	More Details
CVE-2021-37542	In JetBrains TeamCity before 2020.2.3, XSS was possible.	6.1	More Details
CVE-2021-20115	A reflected cross-site scripting vulnerability exists in TCExam <= 14.8.3. The paths provided in the f, d, and dir parameters in tce_filemanager.php were not properly validated and could cause reflected XSS via the unsanitized output of the path supplied. An attacker could craft a malicious link which, if triggered by an administrator, could result in the attacker hijacking the victim's session or performing actions on their behalf.	6.1	More Details
CVE-2021-31655	Cross Site Scripting (XSS) vulnerability in TRENDnet TV-IP110WN V1.2.2.64 V1.2.2.65 V1.2.2.68 via the profile parameter. in a GET request in view.cgi.	6.1	More Details
CVE-2021-22676	UserExcelOut.asp within WebAccess/SCADA is vulnerable to cross-site scripting (XSS), which could allow an attacker to send malicious JavaScript code. This could result in hijacking of cookie/session tokens, redirection to a malicious webpage, and unintended browser action on the WebAccess/SCADA (WebAccess/SCADA versions prior to 8.4.5, WebAccess/SCADA versions prior to 9.0.1).	6.1	More Details
CVE-2021-38157	LeoStream Connection Broker 9.x before 9.0.34.3 allows Unauthenticated Reflected XSS via the /index.pl user parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2018-17865	A cross-site scripting (XSS) vulnerability in SAP J2EE Engine 7.01 allows remote attackers to inject arbitrary web script via the wsdlPath parameter to /ctcprotocol/Protocol. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33702	Under certain conditions, NetWeaver Enterprise Portal, versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode report data. An attacker can craft malicious data and print it to the report. In a successful attack, a victim opens the report, and the malicious script gets executed in the victim's browser, resulting in a Stored Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-33703	Under certain conditions, NetWeaver Enterprise Portal, versions - 7.30, 7.31, 7.40, 7.50, does not sufficiently encode URL parameters. An attacker can craft a malicious link and send it to a victim. A successful attack results in Reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-32768	TYPO3 is an open source PHP based web content management system released under the GNU GPL. In affected versions failing to properly parse, sanitize and encode malicious rich-text content, the content rendering process in the website frontend is vulnerable to cross-site scripting. Corresponding rendering instructions via TypoScript functionality HTMLparser does not consider all potentially malicious HTML tag & attribute combinations per default. In default scenarios, a valid backend user account is needed to exploit this vulnerability. In case custom plugins used in the website frontend accept and reflect rich-text content submitted by users, no authentication is required. Update to TYPO3 versions 7.6.53 ELTS, 8.7.42 ELTS, 9.5.29, 10.4.19, 11.3.2 that fix the problem described.	6.1	More Details
CVE-2021-32596	A use of one-way hash with a predictable salt vulnerability in the password storing mechanism of FortiPortal 6.0.0 through 6.04 may allow an attacker already in possession of the password store to decrypt the passwords by means of precomputed tables.	6.0	More Details
CVE-2021-38370	In Alpine before 2.25, untagged responses from an IMAP server are accepted before STARTTLS.	5.9	More Details
CVE-2021-3678	showdoc is vulnerable to Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	5.9	More Details
CVE-2021-36221	Go before 1.15.15 and 1.16.x before 1.16.7 has a race condition that can lead to a net/http/httputil ReverseProxy panic upon an ErrAbortHandler abort.	5.9	More Details
CVE-2020-36472	An issue was discovered in the max7301 crate before 0.2.0 for Rust. The ImmediateIO and TransactionalIO types implement Sync for all Expander<EI> types that they contain.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36466	An issue was discovered in the cgc crate through 2020-12-10 for Rust. Ptr implements Send and Sync for all types.	5.9	More Details
CVE-2020-36467	An issue was discovered in the cgc crate through 2020-12-10 for Rust. Ptr::get returns more than one mutable reference to the same object.	5.9	More Details
CVE-2020-36468	An issue was discovered in the cgc crate through 2020-12-10 for Rust. Ptr::write performs non-atomic write operations on an underlying pointer.	5.9	More Details
CVE-2021-29969	If Thunderbird was configured to use STARTTLS for an IMAP connection, and an attacker injected IMAP server responses prior to the completion of the STARTTLS handshake, then Thunderbird didn't ignore the injected data. This could have resulted in Thunderbird showing incorrect information, for example the attacker could have tricked Thunderbird to show folders that didn't exist on the IMAP server. This vulnerability affects Thunderbird < 78.12.	5.9	More Details
CVE-2020-36469	An issue was discovered in the appendix crate through 2020-11-15 for Rust. For the generic K and V type parameters, Send and Sync are implemented unconditionally.	5.9	More Details
CVE-2020-36470	An issue was discovered in the disrustor crate through 2020-12-17 for Rust. RingBuffer doe not properly limit the number of mutable references.	5.9	More Details
CVE-2021-38191	An issue was discovered in the tokio crate before 1.8.1 for Rust. Upon a JoinHandle::abort, a Task may be dropped in the wrong thread.	5.9	More Details
CVE-2020-36471	An issue was discovered in the generator crate before 0.7.0 for Rust. It does not ensure that a function (for yielding values) has Send bounds.	5.9	More Details
CVE-2021-32793	Pi-hole's Web interface provides a central location to manage a Pi-hole instance and review performance statistics. Prior to Pi-hole Web interface version 5.5.1, the function to add domains to blocklists or allowlists is vulnerable to a stored cross-site-scripting vulnerability. User input added as a wildcard domain to a blocklist or allowlist is unfiltered in the web interface. Since the payload is stored permanently as a wildcard domain, this is a persistent XSS vulnerability. A remote attacker can therefore attack administrative user accounts through client-side attacks. Pi-hole Web Interface version 5.5.1 contains a patch for this vulnerability.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36584	An issue was discovered in GPAC 1.0.1. There is a heap-based buffer overflow in the function gp_rtp_builder_do_tx3g function in ietf/rtp_pck_3gpp.c, as demonstrated by MP4Box. This can cause a denial of service (DOS).	5.5	More Details
CVE-2021-3679	A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way user uses trace ring buffer in a specific way. Only privileged local users (with CAP_SYS_ADMIN capability) could use this flaw to starve the resources causing denial of service.	5.5	More Details
CVE-2015-7731	SAP Mobile Platform 3.0 SP05 ClientHub allows attackers to obtain the keystream and other sensitive information via the DataVault, aka SAP Security Note 2094830.	5.5	More Details
CVE-2020-22352	The gf_dash_segmenter_probe_input function in GPAC v0.8 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-37616	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A null pointer dereference was found in Exiv2 versions v0.27.4 and earlier. The null pointer dereference is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t` or `-P t`). The bug is fixed in version v0.27.5.	5.5	More Details
CVE-2020-24826	A vulnerability in the elf::section::as_strtab function of Libelfin v0.3 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted ELF file.	5.5	More Details
CVE-2020-24827	A vulnerability in the dwarf::cursor::skip_form function of Libelfin v0.3 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted ELF file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37621	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the image ICC profile, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p C`). The bug is fixed in version v0.27.5.	5.5	More Details
CVE-2021-37622	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when deleting the IPTC data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-d I rm`). The bug is fixed in version v0.27.5.	5.5	More Details
CVE-2021-34334	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.5.	5.5	More Details
CVE-2020-24829	An issue was discovered in GPAC v0.8.0, as demonstrated by MP4Box. It contains a heap-based buffer overflow in gf_m2ts_section_complete in media_tools/mpegts.c that can cause a denial of service (DOS) via a crafted MP4 file.	5.5	More Details
CVE-2021-38114	libavcodec/dnxhddec.c in FFmpeg 4.4 does not check the return value of the init_vlc function, a similar issue to CVE-2013-0868.	5.5	More Details
CVE-2021-25444	An IV reuse vulnerability in keymaster prior to SMR AUG-2021 Release 1 allows decryption of custom keyblob with privileged process.	5.5	More Details
CVE-2021-33717	A vulnerability has been identified in JT2Go (All versions < V13.2.0.1), Teamcenter Visualization (All versions < V13.2.0.1). When parsing specially crafted CGM Files, a NULL pointer deference condition could cause the application to crash. The application must be restarted to restore the service. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23172	A vulnerability in all versions of Kuba allows attackers to overwrite arbitrary files in arbitrary directories with crafted Zip files due to improper validation of file paths in .zip archives.	5.5	More Details
CVE-2021-37178	A vulnerability has been identified in Solid Edge SE2021 (All Versions < SE2021MP7). An XML external entity injection vulnerability in the underlying XML parser could cause the affected application to disclose arbitrary files to remote attackers by loading a specially crafted xml file.	5.5	More Details
CVE-2020-23171	A vulnerability in all versions of Nim-lang allows unauthenticated attackers to write files to arbitrary directories via a crafted zip file with dot-slash characters included in the name of the crafted file.	5.5	More Details
CVE-2021-37623	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An infinite loop was found in Exiv2 versions v0.27.4 and earlier. The infinite loop is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when deleting the IPTC data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-d I rm`). The bug is fixed in version v0.27.5.	5.5	More Details
CVE-2021-37231	A stack-buffer-overflow occurs in Atomicparsley 20210124.204813.840499f through APar_readX() in src/util.cpp while parsing a crafted mp4 file because of the missing boundary check.	5.5	More Details
CVE-2021-32815	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The assertion failure is triggered when Exiv2 is used to modify the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when modifying the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `fi`. ### Patches The bug is fixed in version v0.27.5. ### References Regression test and bug fix: #1739 ### For more information Please see our [security policy](https://github.com/Exiv2/exiv2/security/policy) for information about Exiv2 security.	5.5	More Details
CVE-2021-38206	The mac80211 subsystem in the Linux kernel before 5.12.13, when a device supporting only 5 GHz is used, allows attackers to cause a denial of service (NULL pointer dereference in the radiotap parser) by injecting a frame with 802.11a rates.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21684	A global buffer overflow in the put_font in genpict2e.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into pict2e format.	5.5	More Details
CVE-2020-21683	A global buffer overflow in the shade_or_tint_name_after_declare_color in genpstricks.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into pstricks format.	5.5	More Details
CVE-2020-21682	A global buffer overflow in the set_fill component in genge.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into ge format.	5.5	More Details
CVE-2021-22295	A component of the HarmonyOS has a permission bypass vulnerability. Local attackers may exploit this vulnerability to cause the device to hang due to the page error OsVmPageFaultHandler.	5.5	More Details
CVE-2020-21681	A global buffer overflow in the set_color component in genge.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into ge format.	5.5	More Details
CVE-2020-21680	A stack-based buffer overflow in the put_arrow() component in genpict2e.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into pict2e format.	5.5	More Details
CVE-2020-21678	A global buffer overflow in the genmp_writefontmacro_latex component in genmp.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into mp format.	5.5	More Details
CVE-2020-24825	A vulnerability in the line_table::line_table function of Libelfin v0.3 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted ELF file.	5.5	More Details
CVE-2021-38198	arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a shadow page, leading to a missing guest protection page fault.	5.5	More Details
CVE-2020-21676	A stack-based buffer overflow in the genpstrx_text() component in genpstricks.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into pstricks format.	5.5	More Details
CVE-2021-38200	arch/powerpc/perf/core-book3s.c in the Linux kernel before 5.12.13, on systems with perf_event_paranoid=-1 and no specific PMU driver support registered, allows local users to cause a denial of service (perf_instruction_pointer NULL pointer dereference and OOPS) via a "perf record" command.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3566	Prior to ffmpeg version 4.3, the tty demuxer did not have a 'read_probe' function assigned to it. By crafting a legitimate "ffconcat" file that references an image, followed by a file the triggers the tty demuxer, the contents of the second file will be copied into the output file verbatim (as long as the `-vcodec copy` option is passed to ffmpeg).	5.5	More Details
CVE-2021-38203	btrfs in the Linux kernel before 5.13.4 allows attackers to cause a denial of service (deadlock) via processes that trigger allocation of new system chunks during times when there is a shortage of free space in the system space_info.	5.5	More Details
CVE-2020-21675	A stack-based buffer overflow in the genptk_text component in genptk.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into ptk format.	5.5	More Details
CVE-2020-24822	A vulnerability in the dwarf::cursor::uleb function of Libelfin v0.3 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted ELF file.	5.5	More Details
CVE-2021-21791	An information disclosure vulnerability exists in the the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. The IN instruction can read two bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users.	5.5	More Details
CVE-2020-24821	A vulnerability in the dwarf::cursor::skip_form function of Libelfin v0.3 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted ELF file.	5.5	More Details
CVE-2020-24823	A vulnerability in the dwarf::to_string function of Libelfin v0.3 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted ELF file.	5.5	More Details
CVE-2021-38208	net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL pointer dereference and BUG) by making a getsockname call after a certain type of failure of a bind call.	5.5	More Details
CVE-2021-21785	An information disclosure vulnerability exists in the IOCTL 0x9c40a148 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to a disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21790	An information disclosure vulnerability exists in the the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. The IN instruction can read two bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users.	5.5	More Details
CVE-2020-24824	A global buffer overflow issue in the dwarf::line_table::line_table function of Libelfin v0.3 allows attackers to cause a denial of service (DOS).	5.5	More Details
CVE-2021-21792	An information disclosure vulnerability exists in the the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. The IN instruction can read four bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users.	5.5	More Details
CVE-2021-36454	Cross Site Scripting (XSS) vulnerability in Naviwebs Navigate Cms 2.9 via the navigate-quickse parameter to 1) backups\backups.php, 2) blocks\blocks.php, 3) brands\brands.php, 4) comments\comments.php, 5) coupons\coupons.php, 6) feeds\feeds.php, 7) functions\functions.php, 8) items\items.php, 9) menus\menus.php, 10) orders\orders.php, 11) payment_methods\payment_methods.php, 12) products\products.php, 13) profiles\profiles.php, 14) shipping_methods\shipping_methods.php, 15) templates\templates.php, 16) users\users.php, 17) webdictionary\webdictionary.php, 18) websites\websites.php, and 19) webusers\webusers.php because the initial_url function is built in these files.	5.4	More Details
CVE-2021-37152	Multiple XSS issues exist in Sonatype Nexus Repository Manager 3 before 3.33.0. An authenticated attacker with the ability to add HTML files to a repository could redirect users to Nexus Repository Manager's pages with code modifications.	5.4	More Details
CVE-2020-21930	A stored cross site scripting (XSS) vulnerability in the web_attr_2 field of Eyoucms v1.4.1 allows authenticated attackers to execute arbitrary web scripts or HTML.	5.4	More Details
CVE-2021-38138	OneNav beta 0.9.12 allows XSS via the Add Link feature. NOTE: the vendor's position is that there intentionally is not any XSS protection at present, because the attack risk is largely limited to a compromised account; however, XSS protection is planned for a future release.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21929	A stored cross site scripting (XSS) vulnerability in the web_copyright field of Eyoucms v1.4.1 allows authenticated attackers to execute arbitrary web scripts or HTML.	5.4	More Details
CVE-2020-4707	IBM API Connect 5.0.0.0 through 5.0.8.11 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: 187370.	5.4	More Details
CVE-2020-18693	Cross Site Scripting (XSS) in MineWebCMS v1.7.0 allows remote attackers to execute arbitrary code by injecting malicious code into the 'Title' field of the component '/admin/news'.	5.4	More Details
CVE-2021-36804	Akaunting version 2.1.12 and earlier suffers from a password reset spoofing vulnerability, wherein an attacker can proxy password reset requests through a running Akaunting instance, if that attacker knows the target's e-mail address. This issue was fixed in version 2.1.13 of the product. Please note that this issue is ultimately caused by the defaults provided by the Laravel framework, specifically how proxy headers are handled with respect to multi-tenant implementations. In other words, while this is not technically a vulnerability in Laravel, this default configuration is very likely to lead to practically identical identical vulnerabilities in Laravel projects that implement multi-tenant applications.	5.4	More Details
CVE-2021-37552	In JetBrains YouTrack before 2021.2.17925, stored XSS was possible.	5.4	More Details
CVE-2013-4718	Cross-site scripting (XSS) vulnerability in Open Ticket Request System (OTRS) ITSM 3.0.x before 3.0.9, 3.1.x before 3.1.10, and 3.2.x before 3.2.7 allows remote authenticated users to inject arbitrary web script or HTML via an ITSM ConfigItem search.	5.4	More Details
CVE-2020-21353	A stored cross site scripting (XSS) vulnerability in /admin/snippets.php of GetSimple CMS 3.4.0a allows attackers to execute arbitrary web scripts or HTML via crafted payload in the Edit Snippets module.	5.4	More Details
CVE-2021-33336	Cross-site scripting (XSS) vulnerability in the Journal module's add article menu in Liferay Portal 7.3.0 through 7.3.3, and Liferay DXP 7.1 fix pack 18, and 7.2 fix pack 5 through 7, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_journal_web_portlet_JournalPortlet_name parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37391	A user without privileges in Chamilo LMS 1.11.14 can send an invitation message to another user, e.g., the administrator, through main/social/search.php, main/inc/lib/social.lib.php and steal cookies or execute arbitrary code on the administration side via a stored XSS vulnerability via social network the send invitation feature.	5.4	More Details
CVE-2021-37788	A vulnerability in the web UI of Gurock TestRail v5.3.0.3603 could allow an unauthenticated, remote attacker to affect the integrity of a device via a clickjacking attack. The vulnerability is due to insufficient input validation of iFrame data in HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by sending crafted HTTP packets with malicious iFrame data. A successful exploit could allow the attacker to perform a clickjacking attack where the user is tricked into clicking a malicious link.	5.4	More Details
CVE-2021-38152	index.php/appointment/insert_patient_add_appointment in Chikitsa Patient Management System 2.0.0 allows XSS.	5.4	More Details
CVE-2021-38151	index.php/appointment/todos in Chikitsa Patient Management System 2.0.0 allows XSS.	5.4	More Details
CVE-2021-38149	index.php/admin/add_user in Chikitsa Patient Management System 2.0.0 allows XSS.	5.4	More Details
CVE-2020-22392	Cross Site Scripting (XSS) vulnerability exists in Subrion CMS 4.2.2 when adding a blog and then editing an image file.	5.4	More Details
CVE-2021-37212	The bulletin function of Flygo contains Insecure Direct Object Reference (IDOR) vulnerability. After being authenticated as a general user, remote attackers can manipulate the bulletin ID in specific Url parameters and access and modify bulletin particular content.	5.4	More Details
CVE-2021-38113	In addBouquet in js/bqe.js in OpenWebif (aka e2openplugin-OpenWebif) through 1.4.7, inserting JavaScript into the Add Bouquet feature of the Bouquet Editor (i.e., bouqueteditor/api/addbouquet?name=) leads to Stored XSS.	5.4	More Details
CVE-2021-24014	Multiple instances of improper neutralization of input during web page generation vulnerabilities in FortiSandbox before 4.0.0 may allow an unauthenticated attacker to perform an XSS attack via specifically crafted request parameters.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37211	The bulletin function of Flygo does not filter special characters while a new announcement is added. Remoter attackers can use the vulnerability with general user's credential to inject JavaScript and execute stored XSS attacks.	5.4	More Details
CVE-2021-24509	The Page View Count WordPress plugin before 2.4.9 does not escape the postid parameter of pvc_stats shortcode, allowing users with a role as low as Contributor to perform Stored XSS attacks. A post made by a contributor would still have to be approved by an admin to have the XSS triggered in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability.	5.4	More Details
CVE-2021-24505	The Forms WordPress plugin before 1.12.3 did not sanitise its input fields, leading to Stored Cross-Site scripting issues. The plugin was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) vulnerability within the Forms "Add new" field.	5.4	More Details
CVE-2021-32594	An unrestricted file upload vulnerability in the web interface of FortiPortal 6.0.0 through 6.0.4, 5.3.0 through 5.3.5, 5.2.0 through 5.2.5, and 4.2.2 and earlier may allow a low-privileged user to potentially tamper with the underlying system's files via the upload of specifically crafted files.	5.4	More Details
CVE-2021-26098	An instance of small space of random values in the RPC API of FortiSandbox before 4.0.0 may allow an attacker in possession of a few information pieces about the state of the device to possibly predict valid session IDs.	5.3	More Details
CVE-2021-38373	In KDE KMail 19.12.3 (aka 5.13.3), the SMTP STARTTLS option is not honored (and cleartext messages are sent) unless "Server requires authentication" is checked.	5.3	More Details
CVE-2021-3692	yii2 is vulnerable to Use of Predictable Algorithm in Random Number Generator	5.3	More Details
CVE-2021-38165	Lynx through 2.8.9 mishandles the userinfo subcomponent of a URI, which allows remote attackers to discover cleartext credentials because they may appear in SNI data.	5.3	More Details
CVE-2021-22923	When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20349	IBM Tivoli Workload Scheduler 9.4 and 9.5 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and gain lower level privileges. IBM X-Force ID: 194599.	5.3	More Details
CVE-2021-37546	In JetBrains TeamCity before 2021.1, an insecure key generation mechanism for encrypted properties was used.	5.3	More Details
CVE-2021-37547	In JetBrains TeamCity before 2020.2.4, insufficient checks during file uploading were made.	5.3	More Details
CVE-2021-37551	In JetBrains YouTrack before 2021.2.16363, system user passwords were hashed with SHA-256.	5.3	More Details
CVE-2021-3642	A flaw was found in Wildfly Elytron in versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality.	5.3	More Details
CVE-2021-25448	Improper access control vulnerability in Smart Touch Call prior to version 1.0.0.5 allows arbitrary webpage loading in webview.	5.3	More Details
CVE-2021-25447	Improper access control vulnerability in SmartThings prior to version 1.7.67.25 allows untrusted applications to cause local file inclusion in webview.	5.3	More Details
CVE-2021-25446	Improper access control vulnerability in SmartThings prior to version 1.7.67.25 allows untrusted applications to cause arbitrary webpage loading in webview.	5.3	More Details
CVE-2021-25445	Unprotected component vulnerability in Samsung Internet prior to version 14.2 allows untrusted application to access internal files in Samsung Internet.	5.3	More Details
CVE-2021-25443	A use after free vulnerability in conn_gadget driver prior to SMR AUG-2021 Release 1 allows malicious action by an attacker.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28397	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7 PLCSIM Advanced (All versions > V2 < V4), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (Version V4.4), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions > V2.5 < V2.9.2), SIMATIC S7-1500 Software Controller (All versions > V2.5 < V21.9), TIM 1531 IRC (incl. SIPLUS NET variants) (Version V2.1). Due to an incorrect authorization check in the affected component, an attacker could extract information about access protected PLC program variables over port 102/tcp from an affected device when reading multiple attributes at once.	5.3	More Details
CVE-2021-22925	curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS`in libcurl. This rarely used option is used to send variable=content pairs toTELNET servers.Due to flaw in the option parser for sending `NEW_ENV` variables, libcurlcould be made to pass on uninitialized data from a stack based buffer to theserver. Therefore potentially revealing sensitive internal information to theserver using a clear-text network protocol.This could happen because curl did not call and use sscanf() correctly whenparsing the string provided by the application.	5.3	More Details
CVE-2021-20598	Overly Restrictive Account Lockout Mechanism vulnerability in Mitsubishi Electric MELSEC iQ-R series CPU modules (R08/16/32/120SFCPU all versions, R08/16/32/120PSFCPU all versions) allows a remote unauthenticated attacker to lockout a legitimate user by continuously trying login with incorrect password.	5.3	More Details
CVE-2020-21356	An information disclosure vulnerability in upload.php of PopojiCMS 1.2 leads to physical path disclosure of the host when 'name = "file" is deleted during file uploads.	5.3	More Details
CVE-2021-36805	Akaunting version 2.1.12 and earlier suffers from a persistent (type II) cross-site scripting (XSS) vulnerability in the sales invoice processing component of the application. This issue was fixed in version 2.1.13 of the product.	5.2	More Details
CVE-2021-3680	showdoc is vulnerable to Missing Cryptographic Step	4.9	More Details
CVE-2021-29739	IBM Planning Analytics Local 2.0 could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. X-Force ID: 198846.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24502	The WP Google Map WordPress plugin before 1.7.7 did not sanitise or escape the Map Title before outputting them in the page, leading to a Stored Cross-Site Scripting issue by high privilege users, even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2020-22732	CMS Made Simple (CMSMS) 2.2.14 allows stored XSS via the Extensions > Fie Picker..	4.8	More Details
CVE-2021-33339	Cross-site scripting (XSS) vulnerability in the Fragment module in Liferay Portal 7.2.1 through 7.3.4, and Liferay DXP 7.2 before fix pack 9 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_site_admin_web_portlet_SiteAdminPortlet_name parameter.	4.8	More Details
CVE-2021-37620	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.4 and earlier. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.5.	4.7	More Details
CVE-2021-37618	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.4 and earlier. The out-of-bounds read is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the image ICC profile, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p C`). The bug is fixed in version v0.27.5.	4.7	More Details
CVE-2021-37619	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.4 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.5.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34335	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A floating point exception (FPE) due to an integer divide by zero was found in Exiv2 versions v0.27.4 and earlier. The FPE is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t` or `-P t`). The bug is fixed in version v0.27.5.	4.7	More Details
CVE-2021-37615	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A null pointer dereference was found in Exiv2 versions v0.27.4 and earlier. The null pointer dereference is triggered when Exiv2 is used to print the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when printing the interpreted (translated) data, which is a less frequently used Exiv2 operation that requires an extra command line option (`-p t` or `-P t`). The bug is fixed in version v0.27.5.	4.7	More Details
CVE-2021-32597	Multiple improper neutralization of input during web page generation (CWE-79) in FortiManager and FortiAnalyzer versions 7.0.0, 6.4.5 and below, 6.2.7 and below user interface, may allow a remote authenticated attacker to perform a Stored Cross Site Scripting attack (XSS) by injecting malicious payload in GET parameters.	4.6	More Details
CVE-2021-21739	A ZTE's product of the transport network access layer has a security vulnerability. Because the system does not sufficiently verify the data reliability, attackers could replace an authenticated optical module on the equipment with an unauthenticated one, bypassing system authentication and detection, thus affecting signal transmission. This affects: <ZXCTN 6120H><V5.10.00B24>	4.6	More Details
CVE-2021-32587	An improper access control vulnerability in FortiManager and FortiAnalyzer GUI interface 7.0.0, 6.4.5 and below, 6.2.8 and below, 6.0.11 and below, 5.6.11 and below may allow a remote and authenticated attacker with restricted user profile to retrieve the list of administrative users of other ADOMs and their related configuration.	4.3	More Details
CVE-2021-37554	In JetBrains YouTrack before 2021.3.21051, a user could see boards without having corresponding permissions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32002	Improper Access Control vulnerability in web service of Secomea SiteManager allows local attacker without credentials to gather network information and configuration of the SiteManager. This issue affects: Secomea SiteManager All versions prior to 9.5 on Hardware.	4.3	More Details
CVE-2021-26999	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information when an Active Directory connection fails. The logged information is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	4.3	More Details
CVE-2021-26998	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information that is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	4.3	More Details
CVE-2021-33706	Due to improper input validation in InfraBox, logs can be modified by an authenticated user.	4.3	More Details
CVE-2021-37213	The check-in record page of Flygo contains Insecure Direct Object Reference (IDOR) vulnerability. After being authenticated as a general user, remote attackers can manipulate the employee ID and date in specific parameters to access particular employee’s check-in record.	4.3	More Details
CVE-2021-24018	A buffer underwrite vulnerability in the firmware verification routine of FortiOS before 7.0.1 may allow an attacker located in the adjacent network to potentially execute arbitrary code via a specifically crafted firmware image.	4.3	More Details
CVE-2021-32598	An improper neutralization of CRLF sequences in HTTP headers ('HTTP Response Splitting') vulnerability In FortiManager and FortiAnalyzer GUI 7.0.0, 6.4.6 and below, 6.2.8 and below, 6.0.11 and below, 5.6.11 and below may allow an authenticated and remote attacker to perform an HTTP request splitting attack which gives attackers control of the remaining headers and body of the response.	4.3	More Details
CVE-2021-29974	When network partitioning was enabled, e.g. as a result of Enhanced Tracking Protection settings, a TLS error page would allow the user to override an error on a domain which had specified HTTP Strict Transport Security (which implies that the error should not be override-able.) This issue did not affect the network connections, and they were correctly upgraded to HTTPS automatically. This vulnerability affects Firefox < 90.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1522	A vulnerability in the change password API of Cisco Connected Mobile Experiences (CMX) could allow an authenticated, remote attacker to alter their own password to a value that does not comply with the strong authentication requirements that are configured on an affected device. This vulnerability exists because a password policy check is incomplete at the time a password is changed at server side using the API. An attacker could exploit this vulnerability by sending a specially crafted API request to the affected device. A successful exploit could allow the attacker to change their own password to a value that does not comply with the configured strong authentication requirements.	4.3	More Details
CVE-2021-25954	In “Dolibarr” application, 2.8.1 to 13.0.4 don’t restrict or incorrectly restricts access to a resource from an unauthorized actor. A low privileged attacker can modify the Private Note which only an administrator has rights to do, the affected field is at “/adherents/note.php?id=1” endpoint.	4.3	More Details
CVE-2021-37215	The employee management page of Flygo contains an Insecure Direct Object Reference (IDOR) vulnerability. After being authenticated as a general user, remote attacker can manipulate the user data and then over-write another employee’s user data by specifying that employee’s ID in the API parameter.	4.3	More Details
CVE-2021-22240	Improper access control in GitLab EE versions 13.11.6, 13.12.6, and 14.0.2 allows users to be created via single sign on despite user cap being enabled	4.2	More Details
CVE-2021-21598	Dell Wyse ThinOS, versions 9.0, 9.1, and 9.1 MR1, contain a Sensitive Information Disclosure Vulnerability. An authenticated attacker with physical access to the system could exploit this vulnerability to read sensitive Smartcard data in log files.	3.9	More Details
CVE-2020-25082	An attacker with physical access to Nuvoton Trusted Platform Module (NPCT75x 7.2.x before 7.2.2.0) could extract an Elliptic Curve Cryptography (ECC) private key via a side-channel attack against ECDSA, because of an Observable Timing Discrepancy.	3.8	More Details
CVE-2021-22924	libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on used file systems.The comparison also didn't include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38365	Winner (aka ToneWinner) desktop speakers through 2021-08-09 allow remote attackers to recover speech signals from the power-indicator LED via a telescope and an electro-optical sensor, aka a "Glowworm" attack.	3.7	More Details
CVE-2021-38372	In KDE Trojita 0.7, man-in-the-middle attackers can create new folders because untagged responses from an IMAP server are accepted before STARTTLS.	3.7	More Details
CVE-2021-33597	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine.	3.5	More Details
CVE-2021-33596	Showing the legitimate URL in the address bar while loading the content from other domain. This makes the user believe that the content is served by a legit domain. Exploiting the vulnerability requires the user to click on a specially crafted, seemingly legitimate URL containing an embedded malicious redirect while using F-Secure Safe Browser for iOS.	3.5	More Details
CVE-2021-38205	drivers/net/ethernet/xilinx/xilinx_emaclite.c in the Linux kernel before 5.13.3 makes it easier for attackers to defeat an ASLR protection mechanism because it prints a kernel pointer (i.e., the real IOMEM pointer).	3.3	More Details
CVE-2021-3655	A vulnerability was found in the Linux kernel in versions prior to v5.14-rc1. Missing size validations on inbound SCTP packets may allow the kernel to read uninitialized memory.	3.3	More Details
CVE-2021-33738	A vulnerability has been identified in JT2Go (All versions < V13.2.0.2), Teamcenter Visualization (All versions < V13.2.0.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13405)	3.3	More Details
CVE-2021-38209	net/netfilter/nf_conntrack_standalone.c in the Linux kernel before 5.12.2 allows observation of changes in any net namespace because these changes are leaked into all other net namespaces. This is related to the NF_SYSCTL_CT_MAX, NF_SYSCTL_CT_EXPECT_MAX, and NF_SYSCTL_CT_BUCKETS sysctls.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21740	There is an information leak vulnerability in the digital media player (DMS) of ZTE's residential gateway product. The attacker could insert the USB disk with the symbolic link into the residential gateway, and access unauthorized directory information through the symbolic link, causing information leak.	2.4	More Details
CVE-2020-21690	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-20451. Reason: This candidate is a duplicate of CVE-2020-20451. Notes: All CVE users should reference CVE-2020-20451 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-24741	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-0570. Reason: This candidate is a duplicate of CVE-2020-0570. A typo caused the wrong ID to be used. Notes: All CVE users should reference CVE-2020-0570 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-3591	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details