SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 12 January 2022

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-2021-43779	GLPI is an open source IT Asset Management, issue tracking system and service desk system. The GLPI addressing plugin in versions < 2.9.1 suffers from authenticated Remote Code Execution vulnerability, allowing access to the server's underlying operating system using command injection abuse of functionality. There is no workaround for this issue and users are advised to upgrade or to disable the addressing plugin.	9.9	More Details
CVE-2022-22817	PIL.ImageMath.eval in Pillow before 9.0.0 allows evaluation of arbitrary expressions, such as ones that use the Python exec method. A lambda expression could also be used.	9.8	More Details
CVE-2022-21907	HTTP Protocol Stack Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-21849	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28103	cscms v4.1 allows for SQL injection via the "page_del" function.	9.8	More Details
CVE-2020-28102	cscms v4.1 allows for SQL injection via the "js_del" function.	9.8	More Details
CVE-2021-43297	A deserialization vulnerability existed in dubbo hessian-lite 3.2.11 and its earlier versions, which could lead to malicious code execution. Most Dubbo users use Hessian2 as the default serialization/deserialization protocol, during Hessian catch unexpected exceptions, Hessian will log out some imformation for users, which may cause remote command execution. This issue affects Apache Dubbo Apache Dubbo 2.6.x versions prior to 2.6.12; Apache Dubbo 2.7.x versions prior to 2.7.15; Apache Dubbo 3.0.x versions prior to 3.0.5.	9.8	More Details
CVE-2021-25032	The PublishPress Capabilities WordPress plugin before 2.3.1, PublishPress Capabilities Pro WordPress plugin before 2.3.1 does not have authorisation and CSRF checks when updating the plugin's settings via the init hook, and does not ensure that the options to be updated belong to the plugin. As a result, unauthenticated attackers could update arbitrary blog options, such as the default role and make any new registered user with an administrator role.	9.8	More Details
CVE-2021-24949	The "WP Search Filters" widget of The Plus Addons for Elementor - Pro WordPress plugin before 5.0.7 does not sanitise and escape the option parameter before using it in a SQL statement, which could lead to SQL injection	9.8	More Details
CVE-2022-22847	Formpipe Lasernet before 9.13.3 allows file inclusion in Client Web Services (either by an authenticated attacker, or in a configuration that does not require authentication).	9.8	More Details
CVE-2022-22845	QXIP SIPCAPTURE homer-app before 1.4.28 for HOMER 7.x has the same 167f0db2-f83e-4baa-9736-d56064a5b415 JWT secret key across different customers' installations.	9.8	More Details
CVE-2021-41842	An issue was discovered in AtaLegacySmm in the kernel 5.0 before 05.08.46, 5.1 before 05.16.46, 5.2 before 05.26.46, 5.3 before 05.35.46, 5.4 before 05.43.46, and 5.5 before 05.51.45 in Insyde InsydeH2O. Code execution can occur because the SMI handler lacks a CommBuffer check.	9.8	More Details
CVE-2022-22823	build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22822	addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	9.8	More Details
CVE-2022-22824	defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	9.8	More Details
CVE-2021-45334	Sourcecodester Online Thesis Archiving System 1.0 is vulnerable to SQL Injection. An attacker can bypass admin authentication and gain access to admin panel using SQL Injection	9.8	More Details
CVE-2021-31522	Kylin can receive user input and load any class through Class.forName(...). This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions; Apache Kylin 4 version 4.0.0 and prior versions.	9.8	More Details
CVE-2021-42392	The org.h2.util.JdbcUtils.getConnection method of the H2 database takes as parameters the class name of the driver and URL of the database. An attacker may pass a JNDI driver name and a URL leading to a LDAP or RMI servers, causing remote code execution. This can be exploited through various attack vectors, most notably through the H2 Console which leads to unauthenticated remote code execution.	9.8	More Details
CVE-2021-40010	The bone voice ID TA has a heap overflow vulnerability.Successful exploitation of this vulnerability may result in malicious code execution.	9.8	More Details
CVE-2021-39996	There is a Heap-based buffer overflow vulnerability with the NFC module in smartphones. Successful exploitation of this vulnerability may cause memory overflow.	9.8	More Details
CVE-2021-39993	There is an Integer overflow vulnerability with ACPU in smartphones. Successful exploitation of this vulnerability may cause out-of-bounds access.	9.8	More Details
CVE-2021-23594	All versions of package realms-shim are vulnerable to Sandbox Bypass via a Prototype Pollution attack vector.	9.8	More Details
CVE-2021-23543	All versions of package realms-shim are vulnerable to Sandbox Bypass via a Prototype Pollution attack vector.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22704	The zabbix-agent2 package before 5.4.9-r1 for Alpine Linux sometimes allows privilege escalation to root because the design incorrectly expected that systemd would (in effect) determine part of the configuration.	9.8	More Details
CVE-2021-45003	Laundry Booking Management System 1.0 (Latest) and previous versions are affected by a remote code execution (RCE) vulnerability in profile.php through the "image" parameter that can execute a webshell payload.	9.8	More Details
CVE-2021-46067	In Vehicle Service Management System 1.0 an attacker can steal the cookies leading to Full Account Takeover.	9.8	More Details
CVE-2021-45456	Apache kylin checks the legitimacy of the project before executing some commands with the project name passed in by the user. There is a mismatch between what is being checked and what is being used as the shell command argument in DiagnosisService. This may cause an illegal project name to pass the check and perform the following steps, resulting in a command injection vulnerability. This issue affects Apache Kylin 4.0.0.	9.8	More Details
CVE-2022-22114	In Teedy, versions v1.5 through v1.9 are vulnerable to Reflected Cross-Site Scripting (XSS). The “search term" search functionality is not sufficiently sanitized while displaying the results of the search, which can be leveraged to inject arbitrary scripts. These scripts are executed in a victim’s browser when they enter the crafted URL. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account Takeover of the administrator, by an unauthenticated attacker.	9.6	More Details
CVE-2021-43052	The Realm Server component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, and TIBCO FTL - Enterprise Edition contains an easily exploitable vulnerability that allows authentication bypass due to a hard coded secret used in the default realm server of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.7.2 and below, TIBCO FTL - Developer Edition: versions 6.7.2 and below, and TIBCO FTL - Enterprise Edition: versions 6.7.2 and below.	9.3	More Details
CVE-2022-21669	PuddingBot is a group management bot. In version 0.0.6-b933652 and prior, the bot token is publicly exposed in main.py, making it accessible to malicious actors. The bot token has been revoked and new version is already running on the server. As of time of publication, the maintainers are planning to update code to reflect this change at a later date.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21846	Microsoft Exchange Server Remote Code Execution Vulnerability	9.0	More Details
CVE-2022-21855	Microsoft Exchange Server Remote Code Execution Vulnerability	9.0	More Details
CVE-2022-21901	Windows Hyper-V Elevation of Privilege Vulnerability	9.0	More Details
CVE-2022-22115	In Teedy, versions v1.5 through v1.9 are vulnerable to Stored Cross-Site Scripting (XSS) in the name of a created Tag. Since the Tag name is not being sanitized properly in the edit tag page, a low privileged attacker can store malicious scripts in the name of the Tag. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account Takeover of the administrator, and privileges escalation.	9.0	More Details
CVE-2022-21969	Microsoft Exchange Server Remote Code Execution Vulnerability	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-45033	A vulnerability has been identified in CP-8000 MASTER MODULE WITH I/O -25/+70°C (All versions < V16.20), CP-8000 MASTER MODULE WITH I/O -40/+70°C (All versions < V16.20), CP-8021 MASTER MODULE (All versions < V16.20), CP-8022 MASTER MODULE WITH GPRS (All versions < V16.20). An undocumented debug port uses hard-coded default credentials. If this port is enabled by a privileged user, an attacker aware of the credentials could access an administrative debug shell on the affected device.	8.8	More Details
CVE-2022-22826	nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21857	Active Directory Domain Services Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-43971	A SQL injection vulnerability in /mobile/SelectUsers.jsp in SysAid ITIL 20.4.74 b10 allows a remote authenticated attacker to execute arbitrary SQL commands via the filterText parameter.	8.8	More Details
CVE-2021-37198	A vulnerability has been identified in COMOS V10.2 (All versions only if web components are used), COMOS V10.3 (All versions < V10.3.3.3 only if web components are used), COMOS V10.4 (All versions < V10.4.1 only if web components are used). The COMOS Web component of COMOS uses a flawed implementation of CSRF prevention. An attacker could exploit this vulnerability to perform cross-site request forgery attacks.	8.8	More Details
CVE-2022-21851	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-21850	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-37197	A vulnerability has been identified in COMOS V10.2 (All versions only if web components are used), COMOS V10.3 (All versions < V10.3.3.3 only if web components are used), COMOS V10.4 (All versions < V10.4.1 only if web components are used). The COMOS Web component of COMOS is vulnerable to SQL injections. This could allow an attacker to execute arbitrary SQL statements.	8.8	More Details
CVE-2021-43973	An unrestricted file upload vulnerability in /UploadPsIcon.jsp in SysAid ITIL 20.4.74 b10 allows a remote authenticated attacker to upload an arbitrary file via the file parameter in the HTTP POST body. A successful request returns the absolute, server-side filesystem path of the uploaded file.	8.8	More Details
CVE-2021-21408	Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.	8.8	More Details
CVE-2020-28679	A vulnerability in the showReports module of Zoho ManageEngine Applications Manager before build 14550 allows authenticated attackers to execute a SQL injection via a crafted request.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21840	Microsoft Office Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-25054	The WPcalc WordPress plugin through 2.1 does not sanitize user input into the 'did' parameter and uses it in a SQL statement, leading to an authenticated SQL Injection vulnerability.	8.8	More Details
CVE-2021-25053	The WP Coder WordPress plugin before 2.5.2 within the wow-company admin menu page allows to include() arbitrary file with PHP extension (as well as with data:// or http:// protocols), thus leading to CSRF RCE.	8.8	More Details
CVE-2021-25052	The Button Generator WordPress plugin before 2.3.3 within the wow-company admin menu page allows to include() arbitrary file with PHP extension (as well as with data:// or http:// protocols), thus leading to CSRF RCE.	8.8	More Details
CVE-2021-25051	The Modal Window WordPress plugin before 5.2.2 within the wow-company admin menu page allows to include() arbitrary file with PHP extension (as well as with data:// or http:// protocols), thus leading to CSRF RCE.	8.8	More Details
CVE-2022-22827	storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	8.8	More Details
CVE-2021-34086	In Ultimaker S3 3D printer, Ultimaker S5 3D printer, Ultimaker 3 3D printer S-line through 6.3 and Ultimaker 3 through 5.2.16, the local webserver hosts APIs vulnerable to CSRF. They do not verify incoming requests.	8.8	More Details
CVE-2021-46147	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. MassEditRegex allows CSRF.	8.8	More Details
CVE-2021-43999	Apache Guacamole 1.2.0 and 1.3.0 do not properly validate responses received from a SAML identity provider. If SAML support is enabled, this may allow a malicious user to assume the identity of another Guacamole user.	8.8	More Details
CVE-2021-40002	The Bluetooth module has an out-of-bounds write vulnerability. Successful exploitation of this vulnerability may result in malicious command execution at the remote end.	8.8	More Details
CVE-2022-21922	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21920	Windows Kerberos Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-40000	The Bluetooth module has an out-of-bounds write vulnerability. Successful exploitation of this vulnerability may result in malicious command execution at the remote end.	8.8	More Details
CVE-2022-22825	lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.	8.8	More Details
CVE-2021-46076	Sourcecodester Vehicle Service Management System 1.0 is vulnerable to File upload. An attacker can upload a malicious php file in multiple endpoints it leading to Code Execution.	8.8	More Details
CVE-2021-46164	Zoho ManageEngine Desktop Central before 10.0.662 allows remote code execution by an authenticated user who has complete access to the Reports module.	8.8	More Details
CVE-2021-20048	A Stack-based buffer overflow in the SonicOS SessionID HTTP response header allows a remote authenticated attacker to cause Denial of Service (DoS) and potentially results in code execution in the firewall. This vulnerability affected SonicOS Gen 5, Gen 6 and Gen 7 firmware versions.	8.8	More Details
CVE-2021-20046	A Stack-based buffer overflow in the SonicOS HTTP Content-Length response header allows a remote authenticated attacker to cause Denial of Service (DoS) and potentially results in code execution in the firewall. This vulnerability affected SonicOS Gen 5, Gen 6 and Gen 7 firmware versions.	8.8	More Details
CVE-2022-22111	In DayByDay CRM, version 2.2.0 is vulnerable to missing authorization. Any application user in the application who has update user permission enabled is able to change the password of other users, including the administrator’s. This allows the attacker to gain access to the highest privileged user in the application.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9057	Z-Wave devices based on Silicon Labs 100, 200, and 300 series chipsets do not support encryption, allowing an attacker within radio range to take control of or cause a denial of service to a vulnerable device. An attacker can also capture and replay Z-Wave traffic. Firmware upgrades cannot directly address this vulnerability as it is an issue with the Z-Wave specification for these legacy chipsets. One way to protect against this vulnerability is to use 500 or 700 series chipsets that support Security 2 (S2) encryption. As examples, the Linear WADWAZ-1 version 3.43 and WAPIRZ-1 version 3.43 (with 300 series chipsets) are vulnerable.	8.8	More Details
CVE-2021-1573	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to improper input validation when parsing HTTPS requests. An attacker could exploit this vulnerability by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2021-34704	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to improper input validation when parsing HTTPS requests. An attacker could exploit this vulnerability by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2021-43053	The Realm Server component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, and TIBCO FTL - Enterprise Edition contains a difficult to exploit vulnerability that allows an unauthenticated attacker with network access to obtain the cluster secret of another application connected to the realm server. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.7.2 and below, TIBCO FTL - Developer Edition: versions 6.7.2 and below, and TIBCO FTL - Enterprise Edition: versions 6.7.2 and below.	8.5	More Details
CVE-2022-21837	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44458	Linux users running Lens 5.2.6 and earlier could be compromised by visiting a malicious website. The malicious website could make websocket connections from the victim's browser to Lens and so operate the local terminal feature. This would allow the attacker to execute arbitrary commands as the Lens user.	8.3	More Details
CVE-2021-45971	An issue was discovered in SdHostDriver in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (CommBufferData).	8.2	More Details
CVE-2021-45970	An issue was discovered in IdeBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the status code saved at the CommBuffer+4 location).	8.2	More Details
CVE-2021-45969	An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the CommBuffer+8 location).	8.2	More Details
CVE-2022-21671	@replit/crosis is a JavaScript client that speaks Replit's container protocol. A vulnerability that involves exposure of sensitive information exists in versions prior to 7.3.1. When using this library as a way to programmatically communicate with Replit in a standalone fashion, if there are multiple failed attempts to contact Replit through a WebSocket, the library will attempt to communicate using a fallback poll-based proxy. The URL of the proxy has changed, so any communication done to the previous URL could potentially reach a server that is outside of Replit's control and the token used to connect to the Repl could be obtained by an attacker, leading to full compromise of that Repl (not of the account). This was patched in version 7.3.1 by updating the address of the fallback WebSocket polling proxy to the new one. As a workaround, a user may specify the new address for the polling host (`gp-v2.replit.com`) in the `ConnectArgs`. More information about this workaround is available in the GitHub Security Advisory.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45460	A vulnerability has been identified in SICAM PQ Analyzer (All versions < V3.18). A service is started by an unquoted registry entry. As there are spaces in this path, attackers with write privilege to those directories might be able to plant executables that will run in place of the legitimate process. Attackers might achieve persistence on the system ("backdoors") or cause a denial of service.	8.1	More Details
CVE-2021-29454	Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.	8.1	More Details
CVE-2020-9058	Z-Wave devices based on Silicon Labs 500 series chipsets using CRC-16 encapsulation, including but likely not limited to the Linear LB60Z-1 version 3.5, Dome DM501 version 4.26, and Jasco ZW4201 version 4.05, do not implement encryption or replay protection.	8.1	More Details
CVE-2021-44564	A security vulnerability originally reported in the SYNC2101 product, and applicable to specific sub-families of SYNC devices, allows an attacker to download the configuration file used in the device and apply a modified configuration file back to the device. The attack requires network access to the SYNC device and knowledge of its IP address. The attack exploits the unsecured communication channel used between the administration tool Easyconnect and the SYNC device (in the affected family of SYNC products).	8.1	More Details
CVE-2022-21646	SpiceDB is a database system for managing security-critical application permissions. Any user making use of a wildcard relationship under the right hand branch of an `exclusion` or within an `intersection` operation will see `Lookup`/`LookupResources` return a resource as "accessible" if it is *not* accessible by virtue of the inclusion of the wildcard in the intersection or the right side of the exclusion. In `v1.3.0`, the wildcard is ignored entirely in lookup's dispatch, resulting in the `banned` wildcard being ignored in the exclusion. Version 1.4.0 contains a patch for this issue. As a workaround, don't make use of wildcards on the right side of intersections or within exclusions.	8.1	More Details
CVE-2021-46143	In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43816	containerd is an open source container runtime. On installations using SELinux, such as EL8 (CentOS, RHEL), Fedora, or SUSE MicroOS, with containerd since v1.5.0-beta.0 as the backing container runtime interface (CRI), an unprivileged pod scheduled to the node may bind mount, via hostPath volume, any privileged, regular file on disk for complete read/write access (sans delete). Such is achieved by placing the in-container location of the hostPath volume mount at either `/etc/hosts`, `/etc/hostname`, or `/etc/resolv.conf`. These locations are being relabeled indiscriminately to match the container process-label which effectively elevates permissions for savvy containers that would not normally be able to access privileged host files. This issue has been resolved in version 1.5.9. Users are advised to upgrade as soon as possible.	8.0	More Details
CVE-2022-21668	pipenv is a Python development workflow tool. Starting with version 2018.10.9 and prior to version 2022.1.8, a flaw in pipenv's parsing of requirements files allows an attacker to insert a specially crafted string inside a comment anywhere within a requirements.txt file, which will cause victims who use pipenv to install the requirements file to download dependencies from a package index server controlled by the attacker. By embedding malicious code in packages served from their malicious index server, the attacker can trigger arbitrary remote code execution (RCE) on the victims' systems. If an attacker is able to hide a malicious `--index-url` option in a requirements file that a victim installs with pipenv, the attacker can embed arbitrary malicious code in packages served from their malicious index server that will be executed on the victim's host during installation (remote code execution/RCE). When pip installs from a source distribution, any code in the setup.py is executed by the install process. This issue is patched in version 2022.1.8. The GitHub Security Advisory contains more information about this vulnerability.	8.0	More Details
CVE-2022-21661	WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain way. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this vulnerability.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21662	WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Low-privileged authenticated users (like author) in WordPress core are able to execute JavaScript/perform stored XSS attack, which can affect high-privileged users. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.	8.0	More Details
CVE-2022-22121	In NocoDB, versions 0.81.0 through 0.83.8 are affected by CSV Injection vulnerability (Formula Injection). A low privileged attacker can create a new table to inject payloads in the table rows. When an administrator accesses the User Management endpoint and exports the data as a CSV file and opens it, the payload gets executed.	8.0	More Details
CVE-2022-0121	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hoppscotch hoppscotch/hoppscotch.This issue affects hoppscotch/hoppscotch before 2.1.1.	8.0	More Details
CVE-2022-21893	Remote Desktop Protocol Remote Code Execution Vulnerability	8.0	More Details
CVE-2021-45441	A origin validation error vulnerability in Trend Micro Apex One (on-prem and SaaS) could allow a local attacker drop and manipulate a specially crafted file to issue commands over a certain pipe and elevate to a higher level of privileges. 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-2022-21916	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21895	Windows User Profile Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21917	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21897	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38990	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the mount command which could lead to code execution. IBM X-Force ID: 212952.	7.8	More Details
CVE-2021-43579	A stack-based buffer overflow in image_load_bmp() in HTMLDOC <= 1.9.13 results in remote code execution if the victim converts an HTML document linking to a crafted BMP file.	7.8	More Details
CVE-2022-21842	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21898	DirectX Graphics Kernel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21902	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21908	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21910	Microsoft Cluster Port Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-46165	Zoho ManageEngine Desktop Central before 10.0.662, during startup, launches an executable file from the batch files, but this file's path might not be properly defined.	7.8	More Details
CVE-2021-45231	A link following privilege escalation vulnerability in Trend Micro Apex One (on-prem and SaaS) and Trend Micro Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to create a specially crafted file with arbitrary content which could grant local privilege escalation on the affected system. 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-2021-30360	Users have access to the directory where the installation repair occurs. Since the MS Installer allows regular users to run the repair, an attacker can initiate the installation repair and place a specially crafted EXE in the repair folder which runs with the Check Point Remote Access Client privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21914	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-45440	A unnecessary privilege vulnerability in Trend Micro Apex One and Trend Micro Worry-Free Business Security 10.0 SP1 (on-prem versions only) could allow a local attacker to abuse an impersonation privilege and elevate to a higher level of privileges. 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-2022-21912	DirectX Graphics Kernel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21841	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21858	Windows Bind Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36412	A heap-based buffer overflow vulnerability exists in MP4Box in GPAC 1.0.1 via the gp_rtp_builder_do_mpeg12_video function, which allows attackers to possibly have unspecified other impact via a crafted file in the MP4Box command,	7.8	More Details
CVE-2022-21835	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21852	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21888	Windows Modern Execution Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21878	Windows Geolocation Service Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21884	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21833	Virtual Machine IDE Drive Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36414	A heab-based buffer overflow vulnerability exists in MP4Box in GPAC 1.0.1 via media.c, which allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	7.8	More Details
CVE-2021-38991	IBM AIX 7.0, 7.1, 7.2, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the lscore command which could lead to code execution. IBM X-Force ID: 212953.	7.8	More Details
CVE-2022-21874	Windows Security Center API Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-36409	There is an Assertion `scaling_list_pred_matrix_id_delta==1' failed at sps.cc:925 in libde265 v1.0.8 when decoding file, which allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file or possibly have unspecified other impact.	7.8	More Details
CVE-2022-0128	vim is vulnerable to Out-of-bounds Read	7.8	More Details
CVE-2022-21885	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21836	Windows Certificate Spoofing Vulnerability	7.8	More Details
CVE-2022-22264	Improper sanitization of incoming intent in Dressroom prior to SMR Jan-2022 Release 1 allows local attackers to read and write arbitrary files without permission.	7.7	More Details
CVE-2022-21932	Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21891	Microsoft Dynamics 365 (on-premises) Spoofing Vulnerability	7.6	More Details
CVE-2021-40038	There is a Double free vulnerability in the AOD module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2022-21848	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2021-40039	There is a Null pointer dereference vulnerability in the camera module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2022-21889	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2021-40035	There is a Buffer overflow vulnerability due to a boundary error with the Samba server in the file management module in smartphones. Successful exploitation of this vulnerability may affect function stability.	7.5	More Details
CVE-2021-40032	The bone voice ID TA has a vulnerability in information management,Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-21843	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability	7.5	More Details
CVE-2021-40029	There is a Buffer overflow vulnerability due to a boundary error with the Samba server in the file management module in smartphones. Successful exploitation of this vulnerability may affect function stability.	7.5	More Details
CVE-2021-40028	The eID module has an out-of-bounds memory write vulnerability,Successful exploitation of this vulnerability may affect data integrity.	7.5	More Details
CVE-2021-40027	The bone voice ID TA has a vulnerability in calculating the buffer length,Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-40026	There is a Heap-based buffer overflow vulnerability in the AOD module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40025	The eID module has a vulnerability that causes the memory to be used without being initialized,Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-40022	The weaver module has a vulnerability in parameter type verification,Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-40031	There is a Null pointer dereference vulnerability in the camera module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2022-21880	Windows GDI+ Information Disclosure Vulnerability	7.5	More Details
CVE-2021-45856	Accu-Time Systems MAXIMUS 1.0 telnet service suffers from a remote buffer overflow which causes the telnet service to crash	7.5	More Details
CVE-2021-46149	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. A denial of service (resource consumption) can be accomplished by searching for a very long key in a Language Name Search.	7.5	More Details
CVE-2022-21890	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2021-24948	The Plus Addons for Elementor - Pro WordPress plugin before 5.0.7 does not validate the qvquery parameter of the tp_get_dl_post_info_ajax AJAX action, which could allow unauthenticated users to retrieve sensitive information, such as private and draft posts	7.5	More Details
CVE-2021-44586	An issue was discovered in dst-admin v1.3.0. The product has an unauthorized arbitrary file download vulnerability that can expose sensitive information.	7.5	More Details
CVE-2022-22846	The dnslib package through 0.9.16 for Python does not verify that the ID value in a DNS reply matches an ID value in a query.	7.5	More Details
CVE-2022-21883	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41769	A vulnerability has been identified in SIPROTEC 5 6MD85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 6MD86 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 6MD89 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 6MU85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7KE85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SA82 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7SA86 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SA87 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SD82 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7SD86 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SD87 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SJ81 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7SJ82 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7SJ85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SJ86 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SK82 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7SK85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SL82 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7SL86 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SL87 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SS85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7ST85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7SX85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7UM85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7UT82 devices (CPU variant CP100) (All versions < V8.83), SIPROTEC 5 7UT85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7UT86 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7UT87 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7VE85 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 7VK87 devices (CPU variant CP300) (All versions < V8.83), SIPROTEC 5 Compact 7SX800 devices (CPU variant CP050) (All versions < V8.83). An improper input validation vulnerability in the web server could allow an unauthenticated user to access device information.	7.5	More Details
CVE-2022-22288	Improper authorization vulnerability in Galaxy Store prior to 4.5.36.5 allows remote app installation of the allowlist.	7.5	More Details
CVE-2021-45116	An issue was discovered in Django 2.2 before 2.2.26, 3.2 before 3.2.11, and 4.0 before 4.0.1. Due to leveraging the Django Template Language's variable resolution logic, the dictsort template filter was potentially vulnerable to information disclosure, or an unintended method call, if passed a suitably crafted key.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21904	Windows GDI Information Disclosure Vulnerability	7.5	More Details
CVE-2021-40020	There is an Out-of-bounds array read vulnerability in the security storage module in smartphones. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2022-21667	soketi is an open-source WebSockets server. There is an unhandled case when reading POST requests which results in the server crashing if it could not read the body of a request. In the event that a POST request is sent to any endpoint of the server with an empty body, even unauthenticated with the Pusher Protocol, it will crash the server. All users that run the server are affected by this vulnerability and it's highly recommended to upgrade to the latest patch. There are no workarounds for this issue.	7.5	More Details
CVE-2022-0133	peertube is vulnerable to Improper Access Control	7.5	More Details
CVE-2021-45034	A vulnerability has been identified in CP-8000 MASTER MODULE WITH I/O -25/+70°C (All versions < V16.20), CP-8000 MASTER MODULE WITH I/O -40/+70°C (All versions < V16.20), CP-8021 MASTER MODULE (All versions < V16.20), CP-8022 MASTER MODULE WITH GPRS (All versions < V16.20). The web server of the affected system allows access to logfiles and diagnostic data generated by a privileged user. An unauthenticated attacker could access the files by knowing the corresponding download links.	7.5	More Details
CVE-2022-21911	.NET Framework Denial of Service Vulnerability	7.5	More Details
CVE-2022-0132	peertube is vulnerable to Server-Side Request Forgery (SSRF)	7.5	More Details
CVE-2021-40021	The eID module has an out-of-bounds memory write vulnerability,Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45115	An issue was discovered in Django 2.2 before 2.2.26, 3.2 before 3.2.11, and 4.0 before 4.0.1. UserAttributeSimilarityValidator incurred significant overhead in evaluating a submitted password that was artificially large in relation to the comparison values. In a situation where access to user registration was unrestricted, this provided a potential vector for a denial-of-service attack.	7.5	More Details
CVE-2021-40018	The eID module has a null pointer reference vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-43045	A vulnerability in the .NET SDK of Apache Avro allows an attacker to allocate excessive resources, potentially causing a denial-of-service attack. This issue affects .NET applications using Apache Avro version 1.10.2 and prior versions. Users should update to version 1.11.0 which addresses this issue.	7.5	More Details
CVE-2021-45458	Apache Kylin provides encryption classes PasswordPlaceholderConfigurer to help users encrypt their passwords. In the encryption algorithm used by this encryption class, the cipher is initialized with a hardcoded key and IV. If users use class PasswordPlaceholderConfigurer to encrypt their password and configure it into kylin's configuration file, there is a risk that the password may be decrypted. This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions; Apache Kylin 4 version 4.0.0 and prior versions.	7.5	More Details
CVE-2021-27738	All request mappings in `StreamingCoordinatorController.java` handling `/kylin/api/streaming_coordinator/*` REST API endpoints did not include any security checks, which allowed an unauthenticated user to issue arbitrary requests, such as assigning/unassigning of streaming cubes, creation/modification and deletion of replica sets, to the Kylin Coordinator. For endpoints accepting node details in HTTP message body, unauthenticated (but limited) server-side request forgery (SSRF) can be achieved. This issue affects Apache Kylin Apache Kylin 3 versions prior to 3.1.2.	7.5	More Details
CVE-2021-44351	An arbitrary file read vulnerability exists in NavigateCMS 2.9 via /navigate/navigate_download.php id parameter.	7.5	More Details
CVE-2021-32996	The FANUC R-30iA and R-30iB series controllers are vulnerable to integer coercion errors, which cause the device to crash. A restart is required.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29050	SphinxSearch in Sphinx Technologies Sphinx through 3.1.1 allows directory traversal (in conjunction with CVE-2019-14511) because the mysql client can be used for CALL SNIPPETS and load_file operations on a full pathname (e.g., a file in the /etc directory). NOTE: this is unrelated to CMUSphinx.	7.5	More Details
CVE-2021-38918	IBM PowerVM Hypervisor FW860, FW940, FW950, and FW1010, through a specific sequence of VM management operations could lead to a violation of the isolation between peer VMs. IBM X-Force ID: 210019.	7.5	More Details
CVE-2021-40014	The bone voice ID trusted application (TA) has a heap overflow vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-22569	An issue in protobuf-java allowed the interleaving of com.google.protobuf.UnknownFieldSet fields in such a way that would be processed out of order. A small malicious payload can occupy the parser for several minutes by creating large numbers of short-lived objects that cause frequent, repeated pauses. We recommend upgrading libraries beyond the vulnerable versions.	7.5	More Details
CVE-2021-45457	In Apache Kylin, Cross-origin requests with credentials are allowed to be sent from any origin. This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions; Apache Kylin 4 version 4.0.0 and prior versions.	7.5	More Details
CVE-2021-38921	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 210067.	7.5	More Details
CVE-2021-44878	If an OpenID Connect provider supports the "none" algorithm (i.e., tokens with no signature), pac4j v5.3.0 (and prior) does not refuse it without an explicit configuration on its side or for the "idtoken" response type which is not secure and violates the OpenID Core Specification. The "none" algorithm does not require any signature verification when validating the ID tokens, which allows the attacker to bypass the token validation by injecting a malformed ID token using "none" as the value of "alg" key in the header with an empty signature value.	7.5	More Details
CVE-2021-40011	There is an uncontrolled resource consumption vulnerability in the display module. Successful exploitation of this vulnerability may affect integrity.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5956	An issue was discovered in SdLegacySmm in Insyde InsydeH2O with kernel 5.1 before 05.15.11, 5.2 before 05.25.11, 5.3 before 05.34.11, and 5.4 before 05.42.11. The software SMI handler allows untrusted external input because it does not verify CommBuffer.	7.5	More Details
CVE-2021-38957	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 could disclose sensitive information due to hazardous input validation during QR code generation. IBM X-Force ID: 212040.	7.5	More Details
CVE-2021-39998	There is Vulnerability of APIs being concurrently called for multiple times in HwConnectivityExService a in smartphones. Successful exploitation of this vulnerability may cause the system to crash and restart.	7.5	More Details
CVE-2022-22110	In Daybyday CRM, versions 1.1 through 2.2.0 enforce weak password requirements in the user update functionality. A user with privileges to update his password could change it to a weak password, such as those with a length of a single character. This may allow an attacker to brute-force users' passwords with minimal to no computational effort.	7.5	More Details
CVE-2021-40005	The distributed data service component has a vulnerability in data access control. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-40004	The cellular module has a vulnerability in permission management. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-32998	The FANUC R-30iA and R-30iB series controllers are vulnerable to an out-of-bounds write, which may allow an attacker to remotely execute arbitrary code. INIT START/restore from backup required.	7.4	More Details
CVE-2022-21664	WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.	7.4	More Details
CVE-2022-0129	Uncontrolled search path element vulnerability in McAfee TechCheck prior to 4.0.0.2 allows a local administrator to load their own Dynamic Link Library (DLL) gaining elevation of privileges to system user. This was achieved through placing the malicious DLL in the same directory that the process was run from.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23568	The package extend2 before 1.0.1 are vulnerable to Prototype Pollution via the extend function due to unsafe recursive merge.	7.3	More Details
CVE-2021-24862	The RegistrationMagic WordPress plugin before 5.0.1.6 does not escape user input in its rm_chronos_ajax AJAX action before using it in a SQL statement when duplicating tasks in batches, which could lead to a SQL injection issue	7.2	More Details
CVE-2021-43947	Affected versions of Atlassian Jira Server and Data Center allow remote attackers with administrator privileges to execute arbitrary code via a Remote Code Execution (RCE) vulnerability in the Email Templates feature. This issue bypasses the fix of https://jira.atlassian.com/browse/JSDSERVER-8665. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.	7.2	More Details
CVE-2022-21666	Useful Simple Open-Source CMS (USOC) is a content management system (CMS) for programmers. Versions prior to Pb2.4Bfx3 allowed Sql injection in usersearch.php only for users with administrative privileges. Users should replace the file `admin/pages/useredit.php` with a newer version. USOC version Pb2.4Bfx3 contains a fixed version of `admin/pages/useredit.php`.	7.2	More Details
CVE-2021-46075	A Privilege Escalation vulnerability exists in Sourcecodester Vehicle Service Management System 1.0. Staff account users can access the admin resources and perform CRUD Operations.	7.2	More Details
CVE-2021-46079	An Unrestricted File Upload vulnerability exists in Sourcecodester Vehicle Service Management System 1.0. A remote attacker can upload malicious files leading to Html Injection.	7.2	More Details
CVE-2021-45442	A link following denial-of-service vulnerability in Trend Micro Worry-Free Business Security (on prem only) could allow a local attacker to overwrite arbitrary files in the context of SYSTEM. This is similar to, but not the same as CVE-2021-44024. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.1	More Details
CVE-2021-34087	In Ultimaker S3 3D printer, Ultimaker S5 3D printer, Ultimaker 3 3D printer S-line through 6.3 and Ultimaker 3 through 5.2.16, the local webserver can be used for clickjacking. This includes the settings page.	7.1	More Details
CVE-2022-0144	shelljs is vulnerable to Improper Privilege Management	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43054	The eFTL Server component of TIBCO Software Inc.'s TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contains an easily exploitable vulnerability that allows a low privileged attacker with network access to generate API tokens that can access any other channel with arbitrary permissions. Affected releases are TIBCO Software Inc.'s TIBCO eFTL - Community Edition: versions 6.7.2 and below, TIBCO eFTL - Developer Edition: versions 6.7.2 and below, and TIBCO eFTL - Enterprise Edition: versions 6.7.2 and below.	7.1	More Details
CVE-2021-44024	A link following denial-of-service vulnerability in Trend Micro Apex One (on-prem and SaaS) and Trend Micro Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to overwrite arbitrary files in the context of SYSTEM. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.1	More Details
CVE-2022-21896	Windows DWM Core Library Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21903	Windows GDI Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21862	Windows Application Model Core API Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21834	Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21869	Clipboard User Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21882	Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21881	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21875	Windows Storage Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21873	Tile Data Repository Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21872	Windows Event Tracing Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21871	Microsoft Diagnostics Hub Standard Collector Runtime Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21870	Tablet Windows User Interface Application Core Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21868	Windows Devices Human Interface Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21859	Windows Accounts Control Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21867	Windows Push Notifications Apps Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21866	Windows System Launcher Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21865	Connected Devices Platform Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21864	Windows UI Immersive Server API Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21863	Windows StateRepository API Server file Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21861	Task Flow Data Engine Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21860	Windows AppContracts API Server Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21919	Windows User Profile Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21887	Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21961	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.8	More Details
CVE-2022-21958	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.8	More Details
CVE-2022-21962	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.8	More Details
CVE-2022-21651	Shopware is an open source e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible.	6.8	More Details
CVE-2022-21892	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.8	More Details
CVE-2022-21959	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.8	More Details
CVE-2022-21960	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21663	WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.	6.6	More Details
CVE-2021-37196	A vulnerability has been identified in COMOS V10.2 (All versions only if web components are used), COMOS V10.3 (All versions < V10.3.3.3 only if web components are used), COMOS V10.3 (All versions >= V10.3.3.3 only if web components are used), COMOS V10.4 (All versions < V10.4.1 only if web components are used). The COMOS Web component of COMOS unpacks specially crafted archive files to relative paths. This vulnerability could allow an attacker to store files in any folder accessible by the COMOS Web webservice.	6.5	More Details
CVE-2021-28714	Guest can force Linux netback driver to hog large amounts of kernel memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714)	6.5	More Details
CVE-2021-43972	An unrestricted file copy vulnerability in /UserSelfServiceSettings.jsp in SysAid ITIL 20.4.74 b10 allows a remote authenticated attacker to copy arbitrary files on the server filesystem to the web root (with an arbitrary filename) via the tempFile and fileName parameters in the HTTP POST body.	6.5	More Details
CVE-2021-41767	Apache Guacamole 1.3.0 and older may incorrectly include a private tunnel identifier in the non-private details of some REST responses. This may allow an authenticated user who already has permission to access a particular connection to read from or interact with another user's active use of that same connection.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9059	Z-Wave devices based on Silicon Labs 500 series chipsets using S0 authentication are susceptible to uncontrolled resource consumption leading to battery exhaustion. As an example, the Schlage BE468 version 3.42 door lock is vulnerable and fails open at a low battery level.	6.5	More Details
CVE-2021-46166	Zoho ManageEngine Desktop Central before 10.0.662 allows authenticated users to obtain sensitive information from the database by visiting the Reports page.	6.5	More Details
CVE-2020-9061	Z-Wave devices using Silicon Labs 500 and 700 series chipsets, including but not likely limited to the SiLabs UZB-7 version 7.00, ZooZ ZST10 version 6.04, Aeon Labs ZW090-A version 3.95, and Samsung STH-ETH-200 version 6.04, are susceptible to denial of service via malformed routing messages.	6.5	More Details
CVE-2022-22836	CoreFTP Server before 727 allows directory traversal (for file creation) by an authenticated attacker via ../ in an HTTP PUT request.	6.5	More Details
CVE-2022-21847	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2021-28712	Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28711	Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713	6.5	More Details
CVE-2021-28713	Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713	6.5	More Details
CVE-2021-28715	Guest can force Linux netback driver to hog large amounts of kernel memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714)	6.5	More Details
CVE-2021-4194	bookstack is vulnerable to Improper Access Control	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21672	make-ca is a utility to deliver and manage a complete PKI configuration for workstations and servers. Starting with version 0.9 and prior to version 1.10, make-ca misinterprets Mozilla certdata.txt and treats explicitly untrusted certificates like trusted ones, causing those explicitly untrusted certificates trusted by the system. The explicitly untrusted certificates were used by some CAs already hacked. Hostile attackers may perform a MIM attack exploiting them. Everyone using the affected versions of make-ca should upgrade to make-ca-1.10, and run `make-ca -f -g` as the `root` user to regenerate the trusted store immediately. As a workaround, users may delete the untrusted certificates from /etc/pki/tls and /etc/ssl/certs manually (or by a script), but this is not recommended because the manual changes will be overwritten next time running make-ca to update the trusted anchor.	6.5	More Details
CVE-2022-21915	Windows GDI+ Information Disclosure Vulnerability	6.5	More Details
CVE-2021-46148	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. Some unprivileged users can view confidential information (e.g., IP addresses and User-Agent headers for election traffic) on a testwiki SecurePoll instance.	6.5	More Details
CVE-2022-22816	path_getbbox in path.c in Pillow before 9.0.0 has a buffer over-read during initialization of ImagePath.Path.	6.5	More Details
CVE-2022-22815	path_getbbox in path.c in Pillow before 9.0.0 improperly initializes ImagePath.Path.	6.5	More Details
CVE-2020-9060	Z-Wave devices based on Silicon Labs 500 series chipsets using S2, including but likely not limited to the ZooZ ZST10 version 6.04, ZooZ ZEN20 version 5.03, ZooZ ZEN25 version 5.03, Aeon Labs ZW090-A version 3.95, and Fibaro FGWPB-111 version 4.3, are susceptible to denial of service and resource exhaustion via malformed SECURITY NONCE GET, SECURITY NONCE GET 2, NO OPERATION, or NIF REQUEST messages.	6.5	More Details
CVE-2022-22701	PartKeepr versions up to v1.4.0, loads attachments using a URL while creating a part and allows the use of the 'file://' URI scheme, allowing an authenticated user to read local files.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36774	Apache Kylin allows users to read data from other database systems using JDBC. The MySQL JDBC driver supports certain properties, which, if left unmitigated, can allow an attacker to execute arbitrary code from a hacker-controlled malicious MySQL server within Kylin server processes. This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions.	6.5	More Details
CVE-2020-10137	Z-Wave devices based on Silicon Labs 700 series chipsets using S2 do not adequately authenticate or encrypt FIND_NODE_IN_RANGE frames, allowing a remote, unauthenticated attacker to inject a FIND_NODE_IN_RANGE frame with an invalid random payload, denying service by blocking the processing of upcoming events.	6.5	More Details
CVE-2022-21918	DirectX Graphics Kernel File Denial of Service Vulnerability	6.5	More Details
CVE-2022-0155	follow-redirects is vulnerable to Exposure of Private Personal Information to an Unauthorized Actor	6.5	More Details
CVE-2021-44591	In libming 0.4.8, the parseSWF_DEFINELOSSLESS2 function in util/parser.c lacks a boundary check that would lead to denial-of-service attacks via a crafted SWF file.	6.5	More Details
CVE-2021-44590	In libming 0.4.8, a memory exhaustion vulnerability exist in the function cws2fws in util/main.c. Remote attackers could launch denial of service attacks by submitting a crafted SWF file that exploits this vulnerability.	6.5	More Details
CVE-2021-43946	Affected versions of Atlassian Jira Server and Data Center allow authenticated remote attackers to add administrator groups to filter subscriptions via a Broken Access Control vulnerability in the /secure/EditSubscription.jspa endpoint. The affected versions are before version 8.13.21, and from version 8.14.0 before 8.20.9.	6.5	More Details
CVE-2021-35452	An Incorrect Access Control vulnerability exists in libde265 v1.0.8 due to a SEGV in slice.cc.	6.5	More Details
CVE-2022-21963	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23154	In Lens prior to 5.3.4, custom helm chart configuration creates helm commands from string concatenation of provided arguments which are then executed in the user's shell. Arguments can be provided which cause arbitrary shell commands to run on the system.	6.3	More Details
CVE-2022-21928	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	6.3	More Details
CVE-2021-36737	The input fields of the Apache Pluto UrlTestPortlet are vulnerable to Cross-Site Scripting (XSS) attacks. Users should migrate to version 3.1.1 of the v3-demo-portlet.war artifact	6.1	More Details
CVE-2021-36738	The input fields in the JSP version of the Apache Pluto Applicant MVCBean CDI portlet are vulnerable to Cross-Site Scripting (XSS) attacks. Users should migrate to version 3.1.1 of the applicant-mvcbean-cdi-jsp-portlet.war artifact	6.1	More Details
CVE-2021-36739	The "first name" and "last name" fields of the Apache Pluto 3.1.0 MVCBean JSP portlet maven archetype are vulnerable to Cross-Site Scripting (XSS) attacks.	6.1	More Details
CVE-2021-37195	A vulnerability has been identified in COMOS V10.2 (All versions only if web components are used), COMOS V10.3 (All versions < V10.3.3.3 only if web components are used), COMOS V10.4 (All versions < V10.4.1 only if web components are used). The COMOS Web component of COMOS accepts arbitrary code as attachment to tasks. This could allow an attacker to inject malicious code that is executed when loading the attachment.	6.1	More Details
CVE-2022-21839	Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability	6.1	More Details
CVE-2021-44584	Cross-site scripting (XSS) vulnerability in index.php in emlog version <= pro-1.0.7 allows remote attackers to inject arbitrary web script or HTML via the s parameter.	6.1	More Details
CVE-2021-46163	Kentico Xperience 13.0.44 allows XSS via an XML document to the Media Libraries subsystem.	6.1	More Details
CVE-2022-22268	Incorrect implementation of Knox Guard prior to SMR Jan-2022 Release 1 allows physically proximate attackers to temporary unlock the Knox Guard via Samsung DeX mode.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46144	Roundcube before 1.4.13 and 1.5.x before 1.5.2 allows XSS via an HTML e-mail message with crafted Cascading Style Sheets (CSS) token sequences.	6.1	More Details
CVE-2021-25047	The 10Web Social Photo Feed WordPress plugin before 1.4.29 was affected by a reflected Cross-Site Scripting (XSS) vulnerability in the wdi_apply_changes admin page, allowing an attacker to perform such attack against any logged in users	6.1	More Details
CVE-2020-23986	Github Read Me Stats commit 3c7220e4f7144f6cb068fd433c774f6db47ccb95 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the function renderError.	6.1	More Details
CVE-2022-21954	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.1	More Details
CVE-2021-31589	A cross-site scripting (XSS) vulnerability has been reported and confirmed for BeyondTrust Secure Remote Access Base Software version 6.0.1 and older, which allows the injection of unauthenticated, specially-crafted web requests without proper sanitization.	6.1	More Details
CVE-2020-27428	A DOM-based cross-site scripting (XSS) vulnerability in Scratch-Svg-Renderer v0.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted sb3 file.	6.1	More Details
CVE-2022-0122	forge is vulnerable to URL Redirection to Untrusted Site	6.1	More Details
CVE-2021-44528	A open redirect vulnerability exists in Action Pack >= 6.0.0 that could allow an attacker to craft a "X-Forwarded-Host" headers in combination with certain "allowed host" formats can cause the Host Authorization middleware in Action Pack to redirect users to a malicious website.	6.1	More Details
CVE-2022-21970	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.1	More Details
CVE-2021-25043	The WOOCS WordPress plugin before 1.3.7.3 does not sanitise and escape the custom_prices parameter before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42841	Insta HMS before 12.4.10 is vulnerable to XSS because of improper validation of user-supplied input by multiple scripts. A remote attacker could exploit this vulnerability via a crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.	6.1	More Details
CVE-2021-43055	The eFTL Server component of TIBCO Software Inc.'s TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contains an easily exploitable vulnerability that allows clients to inherit the permissions of the client that initially connected on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO eFTL - Community Edition: versions 6.7.2 and below, TIBCO eFTL - Developer Edition: versions 6.7.2 and below, and TIBCO eFTL - Enterprise Edition: versions 6.7.2 and below.	5.9	More Details
CVE-2022-21653	Jawn is an open source JSON parser. Extenders of the `org.typelevel.jawn.SimpleFacade` and `org.typelevel.jawn.MutableFacade` who don't override `objectContext()` are vulnerable to a hash collision attack which may result in a denial of service. Most applications do not implement these traits directly, but inherit from a library. `jawn-parser-1.3.1` fixes this issue and users are advised to upgrade. For users unable to upgrade override `objectContext()` to use a collision-safe collection.	5.9	More Details
CVE-2022-22707	In lighttpd 1.4.46 through 1.4.63, the mod_extforward_Forwarded function of the mod_extforward plugin has a stack-based buffer overflow (4 bytes representing -1), as demonstrated by remote denial of service (daemon crash) in a non-default configuration. The non-default configuration requires handling of the Forwarded header in a somewhat unusual manner. Also, a 32-bit system is much more likely to be affected than a 64-bit system.	5.9	More Details
CVE-2022-22284	Improper authentication vulnerability in Samsung Internet prior to 16.0.2.19 allows attackers to bypass secret mode password authentication	5.7	More Details
CVE-2021-46045	GPAC 1.0.1 is affected by: Abort failed. The impact is: cause a denial of service (context-dependent).	5.5	More Details
CVE-2021-46052	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::Tuple::validate.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46142	An issue was discovered in uriparser before 0.9.6. It performs invalid free operations in uriNormalizeSyntax.	5.5	More Details
CVE-2021-46141	An issue was discovered in uriparser before 0.9.6. It performs invalid free operations in uriFreeUriMembers and uriMakeOwner.	5.5	More Details
CVE-2021-46038	A Pointer Dereference vulnerability exists in GPAC 1.0.1 in unlink_chunk.isra, which causes a Denial of Service (context-dependent).	5.5	More Details
CVE-2021-46283	nf_tables_newset in net/netfilter/nf_tables_api.c in the Linux kernel before 5.12.13 allows local users to cause a denial of service (NULL pointer dereference and general protection fault) because of the missing initialization for nft_set_elem_expr_alloc. A local user can set a netfilter table expression in their own namespace.	5.5	More Details
CVE-2022-21964	Remote Desktop Licensing Diagnoser Information Disclosure Vulnerability	5.5	More Details
CVE-2021-46055	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::WasmBinaryBuilder::visitRethrow(wasm::Rethrow*).	5.5	More Details
CVE-2021-46054	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::WasmBinaryBuilder::visitRethrow(wasm::Rethrow*).	5.5	More Details
CVE-2021-46051	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the Media_IsSelfContained function, which could cause a Denial of Service. .	5.5	More Details
CVE-2021-46050	A Stack Overflow vulnerability exists in Binaryen 103 via the printf_common function.	5.5	More Details
CVE-2022-21879	Windows Kernel Elevation of Privilege Vulnerability	5.5	More Details
CVE-2021-46053	A Denial of Service vulnerability exists in Binaryen 103. The program terminates with signal SIGKILL.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21838	Windows Cleanup Manager Elevation of Privilege Vulnerability	5.5	More Details
CVE-2021-46049	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the gf_fileio_check function, which could cause a Denial of Service.	5.5	More Details
CVE-2021-46048	A Denial of Service vulnerability exists in Binaryen 104 due to an assertion abort in wasm::WasmBinaryBuilder::readFunctions.	5.5	More Details
CVE-2022-21877	Storage Spaces Controller Information Disclosure Vulnerability	5.5	More Details
CVE-2021-46047	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the gf_hinter_finalize function.	5.5	More Details
CVE-2021-40037	There is a Vulnerability of accessing resources using an incompatible type (type confusion) in the MPTCP subsystem in smartphones. Successful exploitation of this vulnerability may cause the system to crash and restart.	5.5	More Details
CVE-2021-46046	A Pointer Derefernce Vulnerbility exists GPAC 1.0.1 the gf_isom_box_size function, which could cause a Denial of Service (context-dependent).	5.5	More Details
CVE-2022-21876	Win32k Information Disclosure Vulnerability	5.5	More Details
CVE-2022-21899	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability	5.5	More Details
CVE-2021-45832	A Stack-based Buffer Overflow Vulnerability exists in HDF5 1.13.1-1 at at hdf5/src/H5Eint.c, which causes a Denial of Service (context-dependent).	5.5	More Details
CVE-2022-21906	Windows Defender Application Control Security Feature Bypass Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22271	A missing input validation before memory copy in TIMA trustlet prior to SMR Jan-2022 Release 1 allows attackers to copy data from arbitrary memory.	5.5	More Details
CVE-2021-41043	Use after free in tcpslice triggers AddressSanitizer, no other confirmed impact.	5.5	More Details
CVE-2022-22844	LibTIFF 4.3.0 has an out-of-bounds read in _TIFFmemcpy in tif_unix.c in certain situations involving a custom tag and 0x0200 as the second word of the DE field.	5.5	More Details
CVE-2021-46044	A Pointer Dereference Vulnerabilty exists in GPAC 1.0.1via ShiftMetaOffset.isra, which causes a Denial of Service (context-dependent).	5.5	More Details
CVE-2021-46043	A Pointer Dereference Vulnerability exits in GPAC 1.0.1 in the gf_list_count function, which causes a Denial of Service.	5.5	More Details
CVE-2021-46042	A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the _fseeko function, which causes a Denial of Service.	5.5	More Details
CVE-2021-46041	A Segmentation Fault Vulnerability exists in GPAC 1.0.1 via the co64_box_new function, which causes a Denial of Service.	5.5	More Details
CVE-2021-46039	A Pointer Dereference Vulnerabilty exists in GPAC 1.0.1 via the shift_chunk_offsets.part function, which causes a Denial of Service (context-dependent).	5.5	More Details
CVE-2022-0156	vim is vulnerable to Use After Free	5.5	More Details
CVE-2021-45833	A Stack-based Buffer Overflow Vulnerability exists in HDF5 1.13.1-1 via the H5D__create_chunk_file_map_hyper function in /hdf5/src/H5Dchunk.c, which causes a Denial of Service (context-dependent).	5.5	More Details
CVE-2022-21823	A insecure storage of sensitive information vulnerability exists in Ivanti Workspace Control <2021.2 (10.7.30.0) that could allow an attacker with locally authenticated low privileges to obtain key information due to an unspecified attack vector.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46040	A Pointer Dereference Vulnerabilty exists in GPAC 1.0.1 via the finplace_shift_moov_meta_offsets function, which causes a Denial of Servie (context-dependent).	5.5	More Details
CVE-2021-45830	A heap-based buffer overflow vulnerability exists in HDF5 1.13.1-1 via H5F_addr_decode_len in /hdf5/src/H5Fint.c, which could cause a Denial of Service.	5.5	More Details
CVE-2021-44647	Lua v5.4.3 and above are affected by SEGV by type confusion in funcnamefromcode function in ldebug.c which can cause a local denial of service.	5.5	More Details
CVE-2020-25427	A Null pointer dereference vulnerability exits in MP4Box - GPAC version 0.8.0-rev177-g51a8ef874-master via the gf_isom_get_track_id function, which causes a denial of service.	5.5	More Details
CVE-2022-0173	radare2 is vulnerable to Out-of-bounds Read	5.5	More Details
CVE-2021-36408	An issue was discovered in libde265 v1.0.8.There is a Heap-use-after-free in intrapred.h when decoding file using dec265.	5.5	More Details
CVE-2021-36410	A stack-buffer-overflow exists in libde265 v1.0.8 via fallback-motion.cc in function put_epel_hv_fallback when running program dec265.	5.5	More Details
CVE-2021-36411	An issue has been found in libde265 v1.0.8 due to incorrect access control. A SEGV caused by a READ memory access in function derive_boundaryStrength of deblock.cc has occurred. The vulnerability causes a segmentation fault and application crash, which leads to remote denial of service.	5.5	More Details
CVE-2021-45831	A Null Pointer Dereference vulnerability exitgs in GPAC 1.0.1 in MP4Box via __strlen_avx2, which causes a Denial of Service.	5.5	More Details
CVE-2021-45744	A Stored Cross Site Scripting (XSS) vulnerability exists in bludit 3.13.1 via the TAGS section in login panel.	5.4	More Details
CVE-2021-38895	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209563.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45745	A Stored Cross Site Scripting (XSS) vulnerability exists in Bludit 3.13.1 via the About Plugin in login panel.	5.4	More Details
CVE-2022-0157	phoronix-test-suite is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2022-22109	In Daybyday CRM, version 2.2.0 is vulnerable to Stored Cross-Site Scripting (XSS) vulnerability that allows low privileged application users to store malicious scripts in the title field of new tasks. These scripts are executed in a victim's browser when they open the "/tasks" page to view all the tasks.	5.4	More Details
CVE-2022-22116	In Directus, versions 9.0.0-alpha.4 through 9.4.1 are vulnerable to stored Cross-Site Scripting (XSS) vulnerability via SVG file upload in media upload functionality. A low privileged attacker can inject arbitrary javascript code which will be executed in a victim's browser when they open the image URL.	5.4	More Details
CVE-2022-22117	In Directus, versions 9.0.0-alpha.4 through 9.4.1 allow unrestricted file upload of .html files in the media upload functionality, which leads to Cross-Site Scripting vulnerability. A low privileged attacker can upload a crafted HTML file as a profile avatar, and when an admin or another user opens it, the XSS payload gets triggered.	5.4	More Details
CVE-2021-46146	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. The WikibaseMediaInfo component is vulnerable to XSS via the caption fields for a given media file.	5.4	More Details
CVE-2022-21913	Local Security Authority (Domain Policy) Remote Protocol Security Feature Bypass	5.3	More Details
CVE-2021-40009	There is an Out-of-bounds write vulnerability in the AOD module in smartphones. Successful exploitation of this vulnerability may affect service integrity.	5.3	More Details
CVE-2022-21925	Windows BackupKey Remote Protocol Security Feature Bypass Vulnerability	5.3	More Details
CVE-2022-21924	Workstation Service Remote Protocol Security Feature Bypass Vulnerability	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40003	HwPCAssistant has a path traversal vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	5.3	More Details
CVE-2020-15933	A exposure of sensitive information to an unauthorized actor in Fortinet FortiMail versions 6.0.9 and below, FortiMail versions 6.2.4 and below FortiMail versions 6.4.1 and 6.4.0 allows attacker to obtain potentially sensitive software-version information via client-side resources inspection.	5.3	More Details
CVE-2022-22289	Improper access control vulnerability in S Assistant prior to version 7.5 allows attacker to remotely get senstive information.	5.3	More Details
CVE-2022-21670	markdown-it is a Markdown parser. Prior to version 1.3.2, special patterns with length greater than 50 thousand characterss could slow down the parser significantly. Users should upgrade to version 12.3.2 to receive a patch. There are no known workarounds aside from upgrading.	5.3	More Details
CVE-2021-40001	The CaasKit module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause the MeeTime application to be unavailable.	5.3	More Details
CVE-2021-38956	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 could disclose sensitive version information in HTTP response headers that could aid in further attacks against the system. IBM X-Force ID: 212038	5.3	More Details
CVE-2021-45452	Storage.save in Django 2.2 before 2.2.26, 3.2 before 3.2.11, and 4.0 before 4.0.1 allows directory traversal if crafted filenames are directly passed to it.	5.3	More Details
CVE-2021-42748	In Beaver Builder through 2.5.0.3, attackers can bypass the visibility controls protection mechanism via the REST API.	5.3	More Details
CVE-2021-46145	The keyfob subsystem in Honda Civic 2012 vehicles allows a replay attack for unlocking. This is related to a non-expiring rolling code and counter resynchronization.	5.3	More Details
CVE-2021-23218	When running with FIPS mode enabled, Mirantis Container Runtime 20.10.8 leaks memory during TLS Handshakes which could be abused to cause a denial of service.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43974	An issue was discovered in SysAid ITIL 20.4.74 b10. The /enduserreg endpoint is used to register end users anonymously, but does not respect the server-side setting that determines if anonymous users are allowed to register new accounts. Configuring the server-side setting to disable anonymous user registration only hides the client-side registration form. An attacker can still post registration data to create new accounts without prior authentication.	5.3	More Details
CVE-2022-22120	In NocoDB, versions 0.9 to 0.83.8 are vulnerable to Observable Discrepancy in the password-reset feature. When requesting a password reset for a given email address, the application displays an error message when the email isn't registered within the system. This allows attackers to enumerate the registered users' email addresses.	5.3	More Details
CVE-2021-42749	In Beaver Themer, attackers can bypass conditional logic controls (for hiding content) when viewing the post archives. Exploitation requires that a Themer layout is applied to the archives, and that the post excerpt field is not set.	5.3	More Details
CVE-2022-22265	An improper check or handling of exceptional conditions in NPU driver prior to SMR Jan-2022 Release 1 allows arbitrary memory write and code execution.	5.0	More Details
CVE-2021-46073	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Vehicle Service Management System 1.0 via the User List Section in login panel.	4.8	More Details
CVE-2021-46080	A Cross Site Request Forgery (CSRF) vulnerability exists in Vehicle Service Management System 1.0. An successful CSRF attacks leads to Stored Cross Site Scripting Vulnerability.	4.8	More Details
CVE-2021-46150	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. Special:CheckUserLog allows CheckUser XSS because of date mishandling, as demonstrated by an XSS payload in MediaWiki:October.	4.8	More Details
CVE-2021-46068	A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the My Account Section in login panel.	4.8	More Details
CVE-2021-46069	A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Mechanic List Section in login panel.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46070	A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Service Requests Section in login panel.	4.8	More Details
CVE-2021-46071	A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Category List Section in login panel.	4.8	More Details
CVE-2021-46072	A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Service List Section in login panel.	4.8	More Details
CVE-2021-46074	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Vehicle Service Management System 1.0 via the Settings Section in login panel.	4.8	More Details
CVE-2021-46078	An Unrestricted File Upload vulnerability exists in Sourcecodester Vehicle Service Management System 1.0. A remote attacker can upload malicious files leading to a Stored Cross-Site Scripting vulnerability.	4.8	More Details
CVE-2021-40006	Vulnerability of design defects in the security algorithm component. Successful exploitation of this vulnerability may affect confidentiality.	4.6	More Details
CVE-2021-22567	Bidirectional Unicode text can be interpreted and compiled differently than how it appears in editors which can be exploited to get nefarious code passed a code review by appearing benign. An attacker could embed a source that is invisible to a code reviewer that modifies the behavior of a program in unexpected ways.	4.6	More Details
CVE-2022-21900	Windows Hyper-V Security Feature Bypass Vulnerability	4.6	More Details
CVE-2022-21905	Windows Hyper-V Security Feature Bypass Vulnerability	4.6	More Details
CVE-2022-22286	A vulnerability using PendingIntent in Bixby Routines prior to version 3.1.21.8 in Android R(11.0) and 2.6.30.5 in Android Q(10.0) allows attackers to execute privileged action by hijacking and modifying the intent.	4.4	More Details
CVE-2022-21921	Windows Defender Credential Guard Security Feature Bypass Vulnerability	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22285	A vulnerability using PendingIntent in Reminder prior to version 12.2.05.0 in Android R(11.0) and 12.3.02.1000 in Android S(12.0) allows attackers to execute privileged action by hijacking and modifying the intent.	4.4	More Details
CVE-2022-22270	An implicit Intent hijacking vulnerability in Dialer prior to SMR Jan-2022 Release 1 allows unprivileged applications to access contact information.	4.4	More Details
CVE-2022-21894	Secure Boot Security Feature Bypass Vulnerability	4.4	More Details
CVE-2022-22702	PartKeepr versions up to v1.4.0, in the functionality to upload attachments using a URL when creating a part does not validate that requests can be made to local ports, allowing an authenticated user to carry out SSRF attacks and port enumeration.	4.3	More Details
CVE-2022-0174	Improper Validation of Specified Quantity in Input vulnerability in dolibarr dolibarr/dolibarr.	4.3	More Details
CVE-2021-43951	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to view object import configuration details via an Information Disclosure vulnerability in the Create Object type mapping feature. The affected versions are before version 4.21.0.	4.3	More Details
CVE-2022-0170	peertube is vulnerable to Improper Access Control	4.3	More Details
CVE-2021-35247	Serv-U web login screen to LDAP authentication was allowing characters that were not sufficiently sanitized. SolarWinds has updated the input mechanism to perform additional validation and sanitization. Please Note: No downstream affect has been detected as the LDAP servers ignored improper characters. To insure proper input validation is completed in all environments. SolarWinds recommends scheduling an update to the latest version of Serv-U.	4.3	More Details
CVE-2021-22060	In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21642	Discourse is an open source platform for community discussion. In affected versions when composing a message from topic the composer user suggestions reveals whisper participants. The issue has been patched in stable version 2.7.13 and beta version 2.8.0.beta11. There is no workaround for this issue and users are advised to upgrade.	4.3	More Details
CVE-2022-22107	In Daybyday CRM, versions 2.0.0 through 2.2.0 are vulnerable to Missing Authorization. An attacker that has the lowest privileges account (employee type user), can view the appointments of all users in the system including administrators. However, this type of user is not authorized to view the calendar at all.	4.3	More Details
CVE-2021-29701	IBM Engineering Workflow Management 7.0, 7.0.1, and 7.0.2 as well as IBM Rational Team Concert 6.0.6 and 6.0.6.1 could allow an authneticated attacker to obtain sensitive information from build definitions that could aid in further attacks against the system. IBM X-Force ID: 200657.	4.3	More Details
CVE-2022-22108	In Daybyday CRM, versions 2.0.0 through 2.2.0 are vulnerable to Missing Authorization. An attacker that has the lowest privileges account (employee type user), can view the absences of all users in the system including administrators. This type of user is not authorized to view this kind of information.	4.3	More Details
CVE-2021-43949	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to view private objects via a Broken Access Control vulnerability in the Custom Fields feature. The affected versions are before version 4.21.0.	4.3	More Details
CVE-2021-40041	There is a Cross-Site Scripting(XSS) vulnerability in HUAWEI WS318n product when processing network settings. Due to insufficient validation of user input, a local authenticated attacker could exploit this vulnerability by injecting special characters. Successful exploit could cause certain information disclosure. Affected product versions include: WS318n-21 10.0.2.2, 10.0.2.5 and 10.0.2.6.	4.2	More Details
CVE-2021-38674	A cross-site scripting (XSS) vulnerability has been reported to affect QTS, QuTS hero and QuTScloud. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of QTS, QuTS hero and QuTScloud: QuTS hero h4.5.4.1771 build 20210825 and later QTS 4.5.4.1787 build 20210910 and later QuTScloud c4.5.7.1864 and later	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21930	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	4.2	More Details
CVE-2022-21931	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	4.2	More Details
CVE-2022-22272	Improper authorization in TelephonyManager prior to SMR Jan-2022 Release 1 allows attackers to get IMSI without READ_PRIVILEGED_PHONE_STATE permission	4.0	More Details
CVE-2022-22269	Keeping sensitive data in unprotected BluetoothSettingsProvider prior to SMR Jan-2022 Release 1 allows untrusted applications to get a local Bluetooth MAC address.	4.0	More Details
CVE-2022-22267	Implicit Intent hijacking vulnerability in ActivityMetricsLogger prior to SMR Jan-2022 Release 1 allows attackers to get running application information.	4.0	More Details
CVE-2022-22266	(Applicable to China models only) Unprotected WifiEvaluationService in TencentWifiSecurity application prior to SMR Jan-2022 Release 1 allows untrusted applications to get WiFi information without proper permission.	4.0	More Details
CVE-2022-22263	Unprotected dynamic receiver in SecSettings prior to SMR Jan-2022 Release 1 allows untrusted applications to launch arbitrary activity.	4.0	More Details
CVE-2022-22287	Abitrary file access vulnerability in Samsung Email prior to 6.1.60.16 allows attacker to read isolated data in sandbox.	3.9	More Details
CVE-2022-21652	Shopware is an open source e-commerce software platform. In affected versions shopware would not invalidate a user session in the event of a password change. With version 5.7.7 the session validation was adjusted, so that sessions created prior to the latest password change of a customer account can't be used to login with said account. This also means, that upon a password change, all existing sessions for a given customer account are automatically considered invalid. There is no workaround for this issue.	3.5	More Details
CVE-2022-0158	vim is vulnerable to Heap-based Buffer Overflow	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25743	kubectl does not neutralize escape, meta or control sequences contained in the raw data it outputs to a terminal. This includes but is not limited to the unstructured string fields in objects such as Events.	3.0	More Details
CVE-2022-22283	Improper session management vulnerability in Samsung Health prior to 6.20.1.005 prevents logging out from Samsung Health App.	2.8	More Details
CVE-2021-38894	IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 209515.	2.7	More Details
CVE-2021-23173	The affected product is vulnerable to an improper access control, which may allow an authenticated user to gain unauthorized access to sensitive data.	2.6	More Details
CVE-2021-43566	All versions of Samba prior to 4.13.16 are vulnerable to a malicious client using an SMB1 or NFS race to allow a directory to be created in an area of the server file system not exported under the share definition. Note that SMB1 has to be enabled, or the share also available via NFS in order for this attack to succeed.	2.5	More Details
CVE-2022-21929	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2.5	More Details
CVE-2022-22821	NVIDIA NeMo before 1.6.0 contains a vulnerability in ASR WebApp, in which ../ Path Traversal may lead to deletion of any directory when admin privileges are available.	2.0	More Details
CVE-2021-46060	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-46059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-46058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details