SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 March 2021

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-14516	In Rockwell Automation FactoryTalk Services Platform Versions 6.10.00 and 6.11.00, there is an issue with the implementation of the SHA-256 hashing algorithm with FactoryTalk Services Platform that prevents the user password from being hashed properly.	10.0	More Details
CVE-2021-29068	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R6700v3 before 1.0.4.98, R6400v2 before 1.0.4.98, R7000 before 1.0.11.106, R6900P before 1.3.2.124, R7000P before 1.3.2.124, R7900 before 1.0.4.26, R7850 before 1.0.5.60, R8000 before 1.0.4.58, RS400 before 1.5.0.48, R6400 before 1.0.1.62, R6700 before 1.0.2.16, R6900 before 1.0.2.16, MK60 before 1.0.5.102, MR60 before 1.0.5.102, MS60 before 1.0.5.102, CBR40 before 2.5.0.10, R8000P before 1.4.1.62, R7960P before 1.4.1.62, R7900P before 1.4.1.62, RAX15 before 1.0.1.64, RAX20 before 1.0.1.64, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, RAX200 before 1.0.2.102, RAX45 before 1.0.2.64, RAX50 before 1.0.2.64, EX7500 before 1.0.0.68, EAX80 before 1.0.1.62, EAX20 before 1.0.0.36, RBK752 before 3.2.16.6, RBK753 before 3.2.16.6, RBK753S before 3.2.16.6, RBK754 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBK853 before 3.2.16.6, RBK854 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, RBR840 before 3.2.16.6, RBS840 before 3.2.16.6, R6120 before 1.0.0.70, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.76, R6850 before 1.1.0.76, R6350 before 1.1.0.76, R6330 before 1.1.0.76, D7800 before 1.0.1.58, RBK50 before 2.6.1.40, RBR50 before 2.6.1.40, RBS50 before 2.6.1.40, RBK40 before 2.6.1.36, RBR40 before 2.6.1.36, RBS40 before 2.6.1.38, RBK23 before 2.6.1.36, RBR20 before 2.6.1.38, RBS20 before 2.6.1.38, RBK12 before 2.6.1.44, RBK13 before 2.6.1.44, RBK14 before 2.6.1.44, RBK15 before 2.6.1.44, RBR10 before 2.6.1.44, RBS10 before 2.6.1.44, R6800 before 1.2.0.72, R6900v2 before 1.2.0.72, R6700v2 before 1.2.0.72, R7200 before 1.2.0.72, R7350 before 1.2.0.72, R7400 before 1.2.0.72, R7450 before 1.2.0.72, AC2100 before 1.2.0.72, AC2400 before 1.2.0.72, AC2600 before 1.2.0.72, R7800 before 1.0.2.74, R8900 before 1.0.5.24, R9000 before 1.0.5.24, RAX120 before 1.0.1.136, XR450 before 2.3.2.66, XR500 before 2.3.2.66, XR700 before 1.0.1.34, and XR300 before 1.0.3.50.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25289	An issue was discovered in Pillow before 8.1.1. TiffDecode has a heap-based buffer overflow when decoding crafted YCbCr files because of certain interpretation conflicts with LibTIFF in RGBA mode. NOTE: this issue exists because of an incomplete fix for CVE-2020-35654.	9.8	More Details
CVE-2021-24148	A business logic issue in the MStore API WordPress plugin, versions before 3.2.0, had an authentication bypass with Sign In With Apple allowing unauthenticated users to recover an authentication cookie with only an email address.	9.8	More Details
CVE-2021-26295	Apache OFBiz has unsafe deserialization prior to 17.12.06. An unauthenticated attacker can use this vulnerability to successfully take over Apache OFBiz.	9.8	More Details
CVE-2021-28955	git-bug before 0.7.2 has an Uncontrolled Search Path Element. It will execute git.bat from the current directory in certain PATH situations (most often seen on Windows).	9.8	More Details
CVE-2020-13963	SOPlanning before 1.47 has Incorrect Access Control because certain secret key information, and the related authentication algorithm, is public. The key for admin is hardcoded in the installation code, and there is no key for publicsp (which is a guest account).	9.8	More Details
CVE-2019-10196	A flaw was found in http-proxy-agent, prior to version 2.1.0. It was discovered http-proxy-agent passes an auth option to the Buffer constructor without proper sanitization. This could result in a Denial of Service through the usage of all available CPU resources and data exposure through an uninitialized memory leak in setups where an attacker could submit typed input to the auth parameter.	9.8	More Details
CVE-2021-28834	Kramdown before 2.3.1 does not restrict Rouge formatters to the Rouge::Formatters namespace, and thus arbitrary classes can be instantiated.	9.8	More Details
CVE-2020-6577	The IT-Recht Kanzlei plugin in Zen Cart 1.5.6c (German edition) allows itrk-api.php rechtstext_language SQL Injection.	9.8	More Details
CVE-2021-26275	The eslint-fixer package through 0.1.5 for Node.js allows command injection via shell metacharacters to the fix function. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The ozum/eslint-fixer GitHub repository has been intentionally deleted	9.8	More Details
CVE-2021-28794	The unofficial ShellCheck extension before 0.13.4 for Visual Studio Code mishandles shellcheck.executablePath.	9.8	More Details
CVE-2021-23274	The Config UI component of TIBCO Software Inc.'s TIBCO API Exchange Gateway and TIBCO API Exchange Gateway Distribution for TIBCO Silver Fabric contains a vulnerability that theoretically allows an unauthenticated attacker with network access to execute a clickjacking attack on the affected system. A successful attack using this vulnerability does not require human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO API Exchange Gateway: versions 2.3.3 and below and TIBCO API Exchange Gateway Distribution for TIBCO Silver Fabric: versions 2.3.3 and below.	9.8	More Details
CVE-2021-24139	Unvalidated input in the Photo Gallery (10Web Photo Gallery) WordPress plugin, versions before 1.5.55, leads to SQL injection via the frontend/models/model.php bwg_search_x parameter.	9.8	More Details
CVE-2021-22860	EIC e-document system does not perform completed identity verification for sorting and filtering personnel data. The vulnerability allows remote attacker to obtain users' credential information without logging in the system, and further acquire the privileged permissions and execute arbitrary commends.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22859	The users' data querying function of EIC e-document system does not filter the special characters which resulted in remote attackers can inject SQL syntax and execute arbitrary commands without privilege.	9.8	More Details
CVE-2020-11299	Buffer overflow can occur in video while playing the non-standard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2020-11227	Out of bound write while parsing RTT/TTY packet parsing due to lack of check of buffer size before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2020-11192	Out of bound write while parsing SDP string due to missing check on null termination in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2019-18235	Advantech Spectre RT ERT351 Versions 5.1.3 and prior has insufficient login authentication parameters required for the web application may allow an attacker to gain full access using a brute-force password attack.	9.8	More Details
CVE-2021-29071	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBR752 before 3.2.17.12, RBR753 before 3.2.17.12, RBR753S before 3.2.17.12, RBR754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	9.6	More Details
CVE-2021-29082	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBW30 before 2.6.1.4, RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBK754 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK854 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	9.6	More Details
CVE-2021-29079	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-29078	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	9.6	More Details
CVE-2021-29077	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBW30 before 2.6.2.2, RBS40V before 2.6.2.4, RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	9.6	More Details
CVE-2021-29065	NETGEAR RBR850 devices before 3.2.10.11 are affected by authentication bypass.	9.6	More Details
CVE-2021-29066	Certain NETGEAR devices are affected by authentication bypass. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29067	Certain NETGEAR devices are affected by authentication bypass. This affects RBW30 before 2.6.2.2, RBS40V before 2.6.2.4, RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	9.6	More Details
CVE-2021-29076	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2020-11189	Buffer over-read can happen while parsing received SDP values due to lack of NULL termination check on SDP in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details
CVE-2020-11188	Buffer over-read can happen while parsing received SDP values due to lack of NULL termination check on SDP in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details
CVE-2020-11190	Buffer over-read can happen while parsing received SDP values due to lack of NULL termination check on SDP in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details
CVE-2020-11222	Buffer over read while processing MT SMS with maximum length due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile	9.1	More Details
CVE-2021-26990	Cloud Manager versions prior to 3.9.4 are susceptible to a vulnerability that could allow a remote attacker to overwrite arbitrary system files.	9.1	More Details
CVE-2020-11171	Buffer over-read can happen while parsing received SDP values due to lack of NULL termination check on SDP in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details
CVE-2020-11166	Potential out of bound read exception when UE receives unusually large number of padding octets in the beginning of ROHC header in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-28660	rtw_wx_set_scan in drivers/staging/rtl8188eu/os_dep/ioctl_linux.c in the Linux kernel through 5.11.6 allows writing beyond the end of the ->ssid[] array. NOTE: from the perspective of kernel.org releases, CVE IDs are not normally used for drivers/staging/* (unfinished work); however, system integrators may have situations in which a drivers/staging issue is relevant to their own customer base.	8.8	More Details
CVE-2021-24149	Unvalidated input in the Modern Events Calendar Lite WordPress plugin, versions before 5.16.6, did not sanitise the mec[post_id] POST parameter in the mec_fes_form AJAX action when logged in as an author+, leading to an authenticated SQL Injection issue.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28956	The unofficial vscode-sass-lint (aka Sass Lint) extension through 1.0.7 for Visual Studio Code allows attackers to execute arbitrary binaries if the user opens a crafted workspace. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2021-28961	applications/luci-app-ddns/luasrc/model/cbi/ddns/detail.lua in the DDNS package for OpenWrt 19.07 allows remote authenticated users to inject arbitrary commands via POST requests.	8.8	More Details
CVE-2021-24132	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.	8.8	More Details
CVE-2021-24137	Unvalidated input in the Blog2Social WordPress plugin, versions before 6.3.1, lead to SQL Injection in the Re-Share Posts feature, allowing authenticated users to inject arbitrary SQL commands.	8.8	More Details
CVE-2019-10127	A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for BigSQL-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code. An attacker having only the unprivileged Windows account can read arbitrary data directory files, essentially bypassing database-imposed read access limitations. An attacker having only the unprivileged Windows account can also delete certain data directory files.	8.8	More Details
CVE-2021-21627	A cross-site request forgery (CSRF) vulnerability in Jenkins Libvirt Agents Plugin 1.9.0 and earlier allows attackers to stop hypervisor domains.	8.8	More Details
CVE-2020-24994	Stack overflow in the parse_tag function in libass/ass_parse.c in libass before 0.15.0 allows remote attackers to cause a denial of service or remote code execution via a crafted file.	8.8	More Details
CVE-2021-24143	Unvalidated input in the AccessPress Social Icons plugin, versions before 1.8.1, did not sanitise its widget attribute, allowing accounts with post permission, such as author, to perform SQL injections.	8.8	More Details
CVE-2021-28817	The Windows Installation component of TIBCO Software Inc.'s TIBCO Rendezvous and TIBCO Rendezvous Developer Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Rendezvous: versions 8.5.1 and below and TIBCO Rendezvous Developer Edition: versions 8.5.1 and below.	8.8	More Details
CVE-2021-28818	The Rendezvous Routing Daemon (rvrd), Rendezvous Secure Routing Daemon (rvrsd), Rendezvous Secure Daemon (rvsd), Rendezvous Cache (rvcache), Rendezvous Secure C API, Rendezvous Java API, and Rendezvous .Net API components of TIBCO Software Inc.'s TIBCO Rendezvous and TIBCO Rendezvous Developer Edition contain a vulnerability that theoretically allows a low privileged attacker with local access on the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from the affected component searching for run-time artifacts outside of the installation hierarchy. Affected releases are TIBCO Software Inc.'s TIBCO Rendezvous: versions 8.5.1 and below and TIBCO Rendezvous Developer Edition: versions 8.5.1 and below.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28819	The Windows Installation component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, and TIBCO FTL - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.5.0 and below, TIBCO FTL - Developer Edition: versions 6.5.0 and below, and TIBCO FTL - Enterprise Edition: versions 6.5.0 and below.	8.8	More Details
CVE-2021-28820	The FTL Server (tibftlserver), FTL C API, FTL Golang API, FTL Java API, and FTL .Net API components of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, and TIBCO FTL - Enterprise Edition contain a vulnerability that theoretically allows a low privileged attacker with local access on the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from the affected component searching for run-time artifacts outside of the installation hierarchy. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.5.0 and below, TIBCO FTL - Developer Edition: versions 6.5.0 and below, and TIBCO FTL - Enterprise Edition: versions 6.5.0 and below.	8.8	More Details
CVE-2021-20678	SQL injection vulnerability in the Paid Memberships Pro versions prior to 2.5.6 allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors.	8.8	More Details
CVE-2021-28821	The Windows Installation component of TIBCO Software Inc.'s TIBCO Enterprise Message Service, TIBCO Enterprise Message Service - Community Edition, and TIBCO Enterprise Message Service - Developer Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Message Service: versions 8.5.1 and below, TIBCO Enterprise Message Service - Community Edition: versions 8.5.1 and below, and TIBCO Enterprise Message Service - Developer Edition: versions 8.5.1 and below.	8.8	More Details
CVE-2021-28822	The Enterprise Message Service Server (tibemsd), Enterprise Message Service Central Administration (tibemsca), Enterprise Message Service JSON configuration generator (tibemsconf2json), and Enterprise Message Service C API components of TIBCO Software Inc.'s TIBCO Enterprise Message Service, TIBCO Enterprise Message Service - Community Edition, and TIBCO Enterprise Message Service - Developer Edition contain a vulnerability that theoretically allows a low privileged attacker with local access on the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from the affected component searching for run-time artifacts outside of the installation hierarchy. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Message Service: versions 8.5.1 and below, TIBCO Enterprise Message Service - Community Edition: versions 8.5.1 and below, and TIBCO Enterprise Message Service - Developer Edition: versions 8.5.1 and below.	8.8	More Details
CVE-2021-28823	The Windows Installation component of TIBCO Software Inc.'s TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, and TIBCO eFTL - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO eFTL - Community Edition: versions 6.5.0 and below, TIBCO eFTL - Developer Edition: versions 6.5.0 and below, and TIBCO eFTL - Enterprise Edition: versions 6.5.0 and below.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28824	The Windows Installation component of TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition, TIBCO ActiveSpaces - Developer Edition, and TIBCO ActiveSpaces - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO ActiveSpaces - Community Edition: versions 4.5.0 and below, TIBCO ActiveSpaces - Developer Edition: versions 4.5.0 and below, and TIBCO ActiveSpaces - Enterprise Edition: versions 4.5.0 and below.	8.8	More Details
CVE-2021-22864	A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to override environment variables leading to code execution on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.3 and was fixed in 3.0.3, 2.22.9, and 2.21.17. This vulnerability was reported via the GitHub Bug Bounty program.	8.8	More Details
CVE-2021-25265	A malicious website could execute code remotely in Sophos Connect Client before version 2.1.	8.8	More Details
CVE-2021-21355	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 8.7.40, 9.5.25, 10.4.14, 11.1.1, due to the lack of ensuring file extensions belong to configured allowed mime-types, attackers can upload arbitrary data with arbitrary file extensions - however, default _fileDenyPattern_ successfully blocked files like _.htaccess_ or _malicious.php_. Besides that, _UploadedFileReferenceConverter_ transforming uploaded files into proper FileReference domain model objects handles possible file uploads for other extensions as well - given those extensions use the Extbase MVC framework, make use of FileReference items in their direct or inherited domain model definitions and did not implement their own type converter. In case this scenario applies, _UploadedFileReferenceConverter_ accepts any file mime-type and persists files in the default location. In any way, uploaded files are placed in the default location _/fileadmin/user_upload/_, in most scenarios keeping the submitted filename - which allows attackers to directly reference files, or even correctly guess filenames used by other individuals, disclosing this information. No authentication is required to exploit this vulnerability. This is fixed in versions 8.7.40, 9.5.25, 10.4.14, 11.1.1.	8.6	More Details
CVE-2020-25097	An issue was discovered in Squid through 4.13 and 5.x through 5.0.4. Due to improper input validation, it allows a trusted client to perform HTTP Request Smuggling and access services otherwise forbidden by the security controls. This occurs for certain uri_whitespace configuration settings.	8.6	More Details
CVE-2021-29074	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects RBW30 before 2.6.2.2, RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	8.4	More Details
CVE-2021-29081	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects RBW30 before 2.6.2.2, RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29075	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects RBW30 before 2.6.2.2, RBK852 before 3.2.17.12, RBK852 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12.	8.4	More Details
CVE-2021-29070	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-29072	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-21357	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 8.7.40, 9.5.25, 10.4.14, 11.1.1 due to improper input validation, attackers can by-pass restrictions of predefined options and submit arbitrary data in the Form Designer backend module of the Form Framework. In the default configuration of the Form Framework this allows attackers to explicitly allow arbitrary mime-types for file uploads - however, default _fileDenyPattern_ successfully blocked files like _.htaccess_ or _malicious.php_. Besides that, attackers can persist those files in any writable directory of the corresponding TYPO3 installation. A valid backend user account with access to the form module is needed to exploit this vulnerability. This is fixed in versions 8.7.40, 9.5.25, 10.4.14, 11.1.1.	8.3	More Details
CVE-2020-12483	The appstore before 8.12.0.0 exposes some of its components, and the attacker can cause remote download and install apps through carefully constructed parameters.	8.2	More Details
CVE-2021-29080	Certain NETGEAR devices are affected by password reset by an unauthenticated attacker. This affects RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR854 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, CBR40 before 2.5.0.10, R7000 before 1.0.11.116, R6900P before 1.3.2.126, R7900 before 1.0.4.38, R7960P before 1.4.1.66, R8000 before 1.0.4.66, R7900P before 1.4.1.66, R8000P before 1.4.1.66, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, and R7000P before 1.3.2.126.	8.1	More Details
CVE-2021-21387	Wrongthink peer-to-peer, end-to-end encrypted messenger with PeerJS and Axolotl ratchet. In wrongthink from version 2.0.0 and before 2.3.0 there was a set of vulnerabilities causing inadequate encryption strength. Part of the secret identity key was disclosed by the fingerprint used for connection. Additionally, the safety number was improperly calculated. It was computed using part of one of the public identity keys instead of being derived from both public identity keys. This caused issues in computing safety numbers which would potentially be exploitable in the real world. Additionally there was inadequate encryption strength due to use of 1024-bit DSA keys. These issues are all fixed in version 2.3.0.	8.1	More Details
CVE-2021-27221	MikroTik RouterOS 6.47.9 allows remote authenticated ftp users to create or overwrite arbitrary .rsc files via the /export command. NOTE: the vendor's position is that this is intended behavior because of how user policies work	8.1	More Details
CVE-2021-28791	The unofficial SwiftFormat extension before 1.3.7 for Visual Studio Code allows remote attackers to execute arbitrary code by constructing a malicious workspace with a crafted swiftformat.path configuration value that triggers execution upon opening the workspace.	7.8	More Details
CVE-2021-26235	FastStone Image Viewer <= 7.5 is affected by a user mode write access violation near NULL at 0x005bdfc9, triggered when a user opens or views a malformed CUR file that is mishandled by FSViewer.exe. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26237	FastStone Image Viewer <= 7.5 is affected by a user mode write access violation at 0x00402d7d, triggered when a user opens or views a malformed CUR file that is mishandled by FSViewer.exe. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution.	7.8	More Details
CVE-2021-26234	FastStone Image Viewer <= 7.5 is affected by a user mode write access violation at 0x00402d8a, triggered when a user opens or views a malformed CUR file that is mishandled by FSViewer.exe. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution.	7.8	More Details
CVE-2021-26233	FastStone Image Viewer <= 7.5 is affected by a user mode write access violation near NULL at 0x005bdfcb, triggered when a user opens or views a malformed CUR file that is mishandled by FSViewer.exe. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution.	7.8	More Details
CVE-2021-26236	FastStone Image Viewer v.<= 7.5 is affected by a Stack-based Buffer Overflow at 0x005BDF49, affecting the CUR file parsing functionality (BITMAPINFOHEADER Structure, 'BitCount' file format field), that will end up corrupting the Structure Exception Handler (SEH). Attackers could exploit this issue to achieve code execution when a user opens or views a malformed/specially crafted CUR file.	7.8	More Details
CVE-2021-24144	Unvalidated input in the Contact Form 7 Database Addon plugin, versions before 1.2.5.6, was prone to a vulnerability that lets remote attackers inject arbitrary formulas into CSV files.	7.8	More Details
CVE-2021-3141	In Unisys Stealth (core) before 6.0.025.0, the Keycloak password is stored in a recoverable format that might be accessible by a local attacker, who could gain access to the Management Server and change the Stealth configuration.	7.8	More Details
CVE-2021-28789	The unofficial apple/swift-format extension before 1.1.2 for Visual Studio Code allows remote attackers to execute arbitrary code by constructing a malicious workspace with a crafted apple-swift-format.path configuration value that triggers execution upon opening the workspace.	7.8	More Details
CVE-2021-28790	The unofficial SwiftLint extension before 1.4.5 for Visual Studio Code allows remote attackers to execute arbitrary code by constructing a malicious workspace with a crafted swiftlint.path configuration value that triggers execution upon opening the workspace.	7.8	More Details
CVE-2017-20002	The Debian shadow package before 1:4.5-1 for Shadow incorrectly lists pts/0 and pts/1 as physical terminals in /etc/securetty. This allows local users to login as password-less users even if they are connected by non-physical means such as SSH (hence bypassing PAM's nullok_secure configuration). This notably affects environments such as virtual machines automatically generated with a default blank root password, allowing all local users to escalate privileges.	7.8	More Details
CVE-2021-28792	The unofficial Swift Development Environment extension before 2.12.1 for Visual Studio Code allows remote attackers to execute arbitrary code by constructing a malicious workspace with a crafted sourcekit-lsp.serverPath, swift.languageServerPath, swift.path.sourcekite, swift.path.sourcekiteDockerMode, swift.path.swift_driver_bin, or swift.path.shell configuration value that triggers execution upon opening the workspace.	7.8	More Details
CVE-2020-26155	Multiple files and folders in Utimaco SecurityServer 4.20.0.4 and 4.31.1.0. are installed with Read/Write permissions for authenticated users, which allows for binaries to be manipulated by non-administrator users. Additionally, entries are made to the PATH environment variable which, in conjunction with these weak permissions, could enable an attacker to perform a DLL hijacking attack.	7.8	More Details
CVE-2020-11228	Part of RPM region was not protected from xblSec itself due to improper policy and leads to unprivileged access in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11309	Use after free in GPU driver while mapping the user memory to GPU memory due to improper check of referenced memory in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2021-3444	The bpf verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register was known to be 0. A local attacker with the ability to load bpf programs could use this gain out-of-bounds reads in kernel memory leading to information disclosure (kernel memory), and possibly out-of-bounds writes that could potentially lead to code execution. This issue was addressed in the upstream kernel in commit 9b00f1b78809 ("bpf: Fix truncation handling for mod32 dst reg wrt zero") and in Linux stable kernels 5.11.2, 5.10.19, and 5.4.101.	7.8	More Details
CVE-2020-7346	Privilege Escalation vulnerability in McAfee Data Loss Prevention (DLP) for Windows prior to 11.6.100 allows a local, low privileged, attacker through the use of junctions to cause the product to load DLLs of the attacker's choosing. This requires the creation and removal of junctions by the attacker along with sending a specific IOTL command at the correct time.	7.8	More Details
CVE-2021-22314	There is a local privilege escalation vulnerability in some versions of ManageOne. A local authenticated attacker could perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege and compromise the service.	7.8	More Details
CVE-2020-35455	The Taidii Diibear Android application 2.4.0 and all its derivatives allow attackers to obtain user credentials from Shared Preferences and the SQLite database because of insecure data storage.	7.8	More Details
CVE-2021-28953	The unofficial C/C++ Advanced Lint extension before 1.9.0 for Visual Studio Code allows attackers to execute arbitrary binaries if the user opens a crafted repository.	7.8	More Details
CVE-2021-28952	An issue was discovered in the Linux kernel through 5.11.8. The sound/soc/qcom/sdm845.c soundwire device driver has a buffer overflow when an unexpected port ID number is encountered, aka CID-1c668e1c0a0f. (This has been fixed in 5.12-rc4.)	7.8	More Details
CVE-2019-10128	A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for EnterpriseDB-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, this allows a local attacker to read arbitrary data directory files, essentially bypassing database-imposed read access limitations. In plausible non-default configurations, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code.	7.8	More Details
CVE-2020-9367	The MPS Agent in Zoho ManageEngine Desktop Central MSP build MSP build 10.0.486 is vulnerable to DLL Hijacking: dcinventory.exe and dcconfig.exe try to load CSUNSAPI.dll without supplying the complete path. The issue is aggravated because this DLL is missing from the installation, thus making it possible to hijack the DLL and subsequently inject code, leading to an escalation of privilege to NT AUTHORITY\SYSTEM.	7.8	More Details
CVE-2020-26886	Softaculous before 5.5.7 is affected by a code execution vulnerability because of External Initialization of Trusted Variables or Data Stores. This leads to privilege escalation on the local host.	7.8	More Details
CVE-2020-35492	A flaw was found in cairo's image-compositor.c in all versions prior to 1.17.4. This flaw allows an attacker who can provide a crafted input file to cairo's image-compositor (for example, by convincing a user to open a file in an application using cairo, or if an application uses cairo on untrusted input) to cause a stack buffer overflow -> out-of-bounds WRITE. The highest impact from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22665	Rockwell Automation DriveTools SP v5.13 and below and Drives AOP v4.12 and below both contain a vulnerability that a local attacker with limited privileges may be able to exploit resulting in privilege escalation and complete control of the system.	7.8	More Details
CVE-2021-28954	In Chris Walz bit before 1.0.5 on Windows, attackers can run arbitrary code via a .exe file in a crafted repository.	7.8	More Details
CVE-2021-21402	Jellyfin is a Free Software Media System. In Jellyfin before version 10.7.1, with certain endpoints, well crafted requests will allow arbitrary file read from a Jellyfin server's file system. This issue is more prevalent when Windows is used as the host OS. Servers that are exposed to the public Internet are potentially at risk. This is fixed in version 10.7.1. As a workaround, users may be able to restrict some access by enforcing strict security permissions on their filesystem, however, it is recommended to update as soon as possible.	7.7	More Details
CVE-2021-21380	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions of XWiki Platform (and only those with the Ratings API installed), the Rating Script Service expose an API to perform SQL requests without escaping the from and where search arguments. This might lead to an SQL script injection quite easily for any user having Script rights on XWiki. The problem has been patched in XWiki 12.9RC1. The only workaround besides upgrading XWiki would be to uninstall the Ratings API in XWiki from the Extension Manager.	7.7	More Details
CVE-2021-29073	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8000P before 1.4.1.66, MK62 before 1.0.6.110, MR60 before 1.0.6.110, MS60 before 1.0.6.110, R7960P before 1.4.1.66, R7900P before 1.4.1.66, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, and RAX200 before 1.0.3.106.	7.6	More Details
CVE-2021-21383	Wiki.js an open-source wiki app built on Node.js. Wiki.js before version 2.5.191 is vulnerable to stored cross-site scripting through mustache expressions in code blocks. This vulnerability exists due to mustache expressions being parsed by Vue during content injection even though it is contained within a `<pre>` element. By creating a crafted wiki page, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the page is viewed by other users. For an example see referenced GitHub Security Advisory. Commit 5ffa189383dd716f12b56b8cae2ba0d075996cf1 fixes this vulnerability by adding the v-pre directive to all `<pre>` tags during the render.	7.6	More Details
CVE-2021-25291	An issue was discovered in Pillow before 8.1.1. In TiffDecode.c, there is an out-of-bounds read in TiffreadRGBATile via invalid tile boundaries.	7.5	More Details
CVE-2019-14852	A flaw was found in 3scale’s APIcast gateway that enabled the TLS 1.0 protocol. An attacker could target traffic using this weaker protocol and break its encryption, gaining access to unauthorized information. Version shipped in Red Hat 3scale API Management Platform is vulnerable to this issue.	7.5	More Details
CVE-2021-28667	StackStorm before 3.4.1, in some situations, has an infinite loop that consumes all available memory and disk space. This can occur if Python 3.x is used, the locale is not utf-8, and there is an attempt to log Unicode data (from an action or rule name).	7.5	More Details
CVE-2021-28110	/exec in TranzWare e-Commerce Payment Gateway (TWEC PG) before 3.1.27.5 had a vulnerability in its XML parser.	7.5	More Details
CVE-2021-25293	An issue was discovered in Pillow before 8.1.1. There is an out-of-bounds read in SGIRleDecode.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25290	An issue was discovered in Pillow before 8.1.1. In TiffDecode.c, there is a negative-offset memcpy with an invalid size.	7.5	More Details
CVE-2020-13924	In Apache Ambari versions 2.6.2.2 and earlier, malicious users can construct file names for directory traversal and traverse to other directories to download files.	7.5	More Details
CVE-2021-27358	The snapshot feature in Grafana 6.7.3 through 7.4.1 can allow an unauthenticated remote attackers to trigger a Denial of Service via a remote API call if a commonly used configuration is set.	7.5	More Details
CVE-2020-26797	Mediainfo before version 20.08 has a heap buffer overflow vulnerability via MediaInfoLib::File_Gxf::ChooseParser_ChannelGrouping.	7.5	More Details
CVE-2021-23359	This affects all versions of package port-killer. If (attacker-controlled) user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. Running this PoC will cause the command touch success to be executed, leading to the creation of a file called success.	7.5	More Details
CVE-2021-28089	Tor before 0.4.5.7 allows a remote participant in the Tor directory protocol to exhaust CPU resources on a target, aka TROVE-2021-001.	7.5	More Details
CVE-2020-28873	Fluxbb 1.5.11 is affected by a denial of service (DoS) vulnerability by sending an extremely long password via the user login form. When a long password is sent, the password hashing process will result in CPU and memory exhaustion on the server.	7.5	More Details
CVE-2019-19343	A flaw was found in Undertow when using Remoting as shipped in Red Hat Jboss EAP before version 7.2.4. A memory leak in HttpOpenListener due to holding remote connections indefinitely may lead to denial of service. Versions before undertow 2.0.25.SP1 and jboss-remoting 5.0.14.SP1 are believed to be vulnerable.	7.5	More Details
CVE-2020-27827	A flaw was found in multiple versions of OpenvSwitch. Specially crafted LLDP packets can cause memory to be lost when allocating data to handle specific optional TLVs, potentially causing a denial of service. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2020-11226	Out of bound memory read in Data modem while unpacking data due to lack of offset length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2021-27306	An improper access control vulnerability in the JWT plugin in Kong Gateway prior to 2.3.2.0 allows unauthenticated users access to authenticated routes without a valid token JWT.	7.5	More Details
CVE-2021-26935	In WoWonder < 3.1, remote attackers can gain access to the database by exploiting a requests.php?f=search-my-followers SQL Injection vulnerability via the event_id parameter.	7.5	More Details
CVE-2020-17525	Subversion's mod_authz_svn module will crash if the server is using in-repository authz rules with the AuthzSVNReposRelativeAccessFile option and a client sends a request for a non-existing repository URL. This can lead to disruption for users of the service. This issue was fixed in mod_dav_svn+mod_authz_svn servers 1.14.1 and mod_dav_svn+mod_authz_svn servers 1.10.7	7.5	More Details
CVE-2021-28831	decompress_gunzip.c in BusyBox through 1.32.1 mishandles the error bit on the huft_build result pointer, with a resultant invalid free or segmentation fault, via malformed gzip data.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11218	Denial of service in baseband when NW configures LTE betaOffset-RI-Index due to lack of data validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-26991	Cloud Manager versions prior to 3.9.4 contain an insecure Cross-Origin Resource Sharing (CORS) policy which could allow a remote attacker to interact with Cloud Manager.	7.5	More Details
CVE-2021-27292	ua-parser-js >= 0.7.14, fixed in 0.7.24, uses a regular expression which is vulnerable to denial of service. If an attacker sends a malicious User-Agent header, ua-parser-js will get stuck processing it for an extended period of time.	7.5	More Details
CVE-2021-27291	In pygments 1.1+, fixed in 2.7.4, the lexers used to parse programming languages rely heavily on regular expressions. Some of the regular expressions have exponential or cubic worst-case complexity and are vulnerable to ReDoS. By crafting malicious input, an attacker can cause a denial of service.	7.5	More Details
CVE-2021-21341	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is vulnerability which may allow a remote attacker to allocate 100% CPU time on the target system depending on CPU type or parallel execution of such a payload resulting in a denial of service only by manipulating the processed input stream. No user is affected who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	7.5	More Details
CVE-2019-18231	Advantech Spectre RT ERT351 Versions 5.1.3 and prior logins and passwords are transmitted in clear text form, which may allow an attacker to intercept the request.	7.5	More Details
CVE-2021-22320	There is a denial of service vulnerability in Huawei products. A module cannot deal with specific messages correctly. Attackers can exploit this vulnerability by sending malicious messages to an affected module. This can lead to denial of service. Affected product include some versions of IPS Module, NGFW Module, NIP6600, NIP6800, Secospace USG6300, Secospace USG6500 and Secospace USG6600.	7.5	More Details
CVE-2021-26578	A potential security vulnerability has been identified in HPE Network Orchestrator (NetO) version(s): Prior to 2.5. The vulnerability could be remotely exploited with SQL injection.	7.5	More Details
CVE-2021-22309	There is insecure algorithm vulnerability in Huawei products. A module uses less random input in a secure mechanism. Attackers can exploit this vulnerability by brute forcing to obtain sensitive message. This can lead to information leak. Affected product versions include:USG9500 versions V500R001C30SPC200, V500R001C60SPC500,V500R005C00SPC200;USG9520 versions V500R005C00;USG9560 versions V500R005C00;USG9580 versions V500R005C00.	7.5	More Details
CVE-2020-9213	There is a denial of service vulnerability in some huawei products. In specific scenarios, due to the improper handling of the packets, an attacker may craft many specific packets. Successful exploit may cause some services to be abnormal. Affected products include some versions of NGFW Module, NIP6300, NIP6600, NIP6800, Secospace USG6300, Secospace USG6500, Secospace USG6600 and SG9500.	7.5	More Details
CVE-2021-28148	One of the usage insights HTTP API endpoints in Grafana Enterprise 6.x before 6.7.6, 7.x before 7.3.10, and 7.4.x before 7.4.5 is accessible without any authentication. This allows any unauthenticated user to send an unlimited number of requests to the endpoint, leading to a denial of service (DoS) attack against a Grafana Enterprise instance.	7.5	More Details
CVE-2021-23360	This affects the package killport before 1.0.2. If (attacker-controlled) user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. Running this PoC will cause the command touch success to be executed, leading to the creation of a file called success.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20222	A flaw was found in keycloak. The new account console in keycloak can allow malicious code to be executed using the referrer URL. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.5	More Details
CVE-2021-28117	libdiscover/backends/KNSBackend/KNSResource.cpp in KDE Discover before 5.21.3 automatically creates links to potentially dangerous URLs (that are neither https:// nor http://) based on the content of the store.kde.org web site. (5.18.7 is also a fixed version.)	7.5	More Details
CVE-2021-21267	Schema-Inspector is an open-source tool to sanitize and validate JS objects (npm package schema-inspector). In before version 2.0.0, email address validation is vulnerable to a denial-of-service attack where some input (for example `a@0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.`) will freeze the program or web browser page executing the code. This affects any current schema-inspector users using any version to validate email addresses. Users who do not do email validation, and instead do other types of validation (like string min or max length, etc), are not affected. Users should upgrade to version 2.0.0, which uses a regex expression that isn't vulnerable to ReDoS.	7.5	More Details
CVE-2021-20270	An infinite loop in SMLLexer in Pygments versions 1.5 to 2.7.3 may lead to denial of service when performing syntax highlighting of a Standard ML (SML) source file, as demonstrated by input that only contains the "exception" keyword.	7.5	More Details
CVE-2021-26992	Cloud Manager versions prior to 3.9.4 are susceptible to a vulnerability which could allow a remote attacker to cause a Denial of Service (DoS).	7.5	More Details
CVE-2021-24146	Lack of authorisation checks in the Modern Events Calendar Lite WordPress plugin, versions before 5.16.5, did not properly restrict access to the export files, allowing unauthenticated users to exports all events data in CSV or XML format for example.	7.5	More Details
CVE-2021-29069	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects XR450 before 2.3.2.114, XR500 before 2.3.2.114, and WNR2000v5 before 1.0.0.76.	7.3	More Details
CVE-2020-28503	The package copy-props before 2.0.5 are vulnerable to Prototype Pollution via the main functionality.	7.3	More Details
CVE-2021-1287	A vulnerability in the web-based management interface of Cisco RV132W ADSL2+ Wireless-N VPN Routers and Cisco RV134W VDSL2 Wireless-AC VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device or cause the device to restart unexpectedly. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition on the affected device.	7.2	More Details
CVE-2019-10200	A flaw was discovered in OpenShift Container Platform 4 where, by default, users with access to create pods also have the ability to schedule workloads on master nodes. Pods with permission to access the host network, running on master nodes, can retrieve security credentials for the master AWS IAM role, allowing management access to AWS resources. With access to the security credentials, the user then has access to the entire infrastructure. Impact to data and system availability is high.	7.2	More Details
CVE-2021-24123	Arbitrary file upload in the PowerPress WordPress plugin, versions before 8.3.8, did not verify some of the uploaded feed images (such as the ones from Podcast Artwork section), allowing high privilege accounts (admin+) being able to upload arbitrary files, such as php, leading to RCE.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27928	A remote code execution issue was discovered in MariaDB 10.2 before 10.2.37, 10.3 before 10.3.28, 10.4 before 10.4.18, and 10.5 before 10.5.9; Percona Server through 2021-03-03; and the wsrep patch through 2021-03-03 for MySQL. An untrusted search path leads to eval injection, in which a database SUPER user can execute OS commands after modifying wsrep_provider and wsrep_notify_cmd. NOTE: this does not affect an Oracle product.	7.2	More Details
CVE-2021-24125	Unvalidated input in the Contact Form Submissions WordPress plugin before 1.7.1, could lead to SQL injection in the wpcf7_contact_form GET parameter when submitting a filter request as a high privilege user (admin+)	7.2	More Details
CVE-2021-28419	The "order_col" parameter in archive.php of SEO Panel 4.8.0 is vulnerable to time-based blind SQL injection, which leads to the ability to retrieve all databases.	7.2	More Details
CVE-2021-24145	Arbitrary file upload in the Modern Events Calendar Lite WordPress plugin, versions before 5.16.5, did not properly check the imported file, allowing PHP ones to be uploaded by administrator by using the 'text/csv' content-type in the request.	7.2	More Details
CVE-2021-24142	Unvaludated input in the 301 Redirects - Easy Redirect Manager WordPress plugin, versions before 2.51, did not sanitise its "Redirect From" column when importing a CSV file, allowing high privilege users to perform SQL injections.	7.2	More Details
CVE-2021-24140	Unvalidated input in the Ajax Load More WordPress plugin, versions before 5.3.2, lead to SQL Injection in POST /wp-admin/admin-ajax.php with param repeater=' or sleep(5)#&type=test.	7.2	More Details
CVE-2021-24130	Unvalidated input in the WP Google Map Plugin WordPress plugin, versions before 4.1.5, in the Manage Locations page within the plugin settings was vulnerable to SQL Injection through a high privileged user (admin+).	7.2	More Details
CVE-2021-24131	Unvalidated input in the Anti-Spam by CleanTalk WordPress plugin, versions before 5.149, lead to multiple authenticated SQL injection vulnerabilities, however, it requires high privilege user (admin+).	7.2	More Details
CVE-2021-24141	Unvaludated input in the Advanced Database Cleaner plugin, versions before 3.0.2, lead to SQL injection allowing high privilege users (admin+) to perform SQL attacks.	7.2	More Details
CVE-2021-26070	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to evade behind-the-firewall protection of app-linked resources via a Broken Authentication vulnerability in the `makeRequest` gadget resource. The affected versions are before version 8.13.3, and from version 8.14.0 before 8.14.1.	7.2	More Details
CVE-2021-22311	There is an improper permission assignment vulnerability in Huawei ManageOne product. Due to improper security hardening, the process can run with a higher privilege. Successful exploit could allow certain users to do certain operations with improper permissions. Affected product versions include: ManageOne versions 8.0.0, 8.0.1.	7.2	More Details
CVE-2021-21401	Nanopb is a small code-size Protocol Buffers implementation in ansi C. In Nanopb before versions 0.3.9.8 and 0.4.5, decoding a specifically formed message can cause invalid `free()` or `realloc()` calls if the message type contains an `oneof` field, and the `oneof` directly contains both a pointer field and a non-pointer field. If the message data first contains the non-pointer field and then the pointer field, the data of the non-pointer field is incorrectly treated as if it was a pointer value. Such message data rarely occurs in normal messages, but it is a concern when untrusted data is parsed. This has been fixed in versions 0.3.9.8 and 0.4.5. See referenced GitHub Security Advisory for more information including workarounds.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27962	Grafana Enterprise 7.2.x and 7.3.x before 7.3.10 and 7.4.x before 7.4.5 allows a dashboard editor to bypass a permission check concerning a data source they should not be able to access.	7.1	More Details
CVE-2020-11290	Use after free condition in msm ioctl events due to race between the ioctl register and deregister events in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.0	More Details
CVE-2021-22848	HGiga MailSherlock contains a SQL Injection. Remote attackers can inject SQL syntax and execute SQL commands in a URL parameter of email pages without privilege.	7.0	More Details
CVE-2020-35454	The Taidii Diibear Android application 2.4.0 and all its derivatives allow attackers to obtain user credentials from an Android backup because of insecure application configuration.	6.8	More Details
CVE-2020-11305	Integer overflow in boot due to improper length check on arguments received in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	6.8	More Details
CVE-2020-11308	Buffer overflow occurs when trying to convert ASCII string to Unicode string if the actual size is more than required in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.8	More Details
CVE-2020-9206	The eUDC660 product has a resource management vulnerability. An attacker with high privilege needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper resource management of the device, as a result, the key file can be obtained and data can be decrypted, affecting confidentiality, integrity, and availability of the device.	6.7	More Details
CVE-2021-28972	In drivers/pci/hotplug/rpadlpar_sysfs.c in the Linux kernel through 5.11.8, the RPA PCI Hotplug driver has a user-tolerable buffer overflow when writing a new device name to the driver from userspace, allowing userspace to write data to the kernel stack frame directly. This occurs because add_slot_store and remove_slot_store mishandle drc_name '\0' termination, aka CID-cc7a0bb058b8.	6.7	More Details
CVE-2021-20077	Nessus Agent versions 7.2.0 through 8.2.2 were found to inadvertently capture the IAM role security token on the local host during initial linking of the Nessus Agent when installed on an Amazon EC2 instance. This could allow a privileged attacker to obtain the token.	6.7	More Details
CVE-2021-20675	M-System DL8 series (type A (DL8-A) versions prior to Ver3.0, type B (DL8-B) versions prior to Ver3.0, type C (DL8-C) versions prior to Ver3.0, type D (DL8-D) versions prior to Ver3.0, and type E (DL8-E) versions prior to Ver3.0) allows remote authenticated attackers to cause a denial of service (DoS) condition via unspecified vectors.	6.5	More Details
CVE-2021-28653	The iOS and macOS apps before 1.4.1 for the Western Digital G-Technology ArmorLock NVMe SSD store keys insecurely. They choose a non-preferred storage mechanism if the device has Secure Enclave support but lacks biometric authentication hardware.	6.5	More Details
CVE-2021-28146	The team sync HTTP API in Grafana Enterprise 7.4.x before 7.4.5 has an Incorrect Access Control issue. On Grafana instances using an external authentication service, this vulnerability allows any authenticated user to add external groups to existing teams. This can be used to grant a user team permissions that the user isn't supposed to have.	6.5	More Details
CVE-2021-25920	In OpenEMR, versions v2.7.2-rc1 to 6.0.0 are vulnerable to Improper Access Control when creating a new user, which leads to a malicious user able to read and send sensitive messages on behalf of the victim user.	6.5	More Details
CVE-2021-25292	An issue was discovered in Pillow before 8.1.1. The PDF parser allows a regular expression DoS (ReDoS) attack via a crafted PDF file because of a catastrophic backtracking regex.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14851	A denial of service vulnerability was discovered in nbdkit. A client issuing a certain sequence of commands could possibly trigger an assertion failure, causing nbdkit to exit. This issue only affected nbdkit versions 1.12.7, 1.14.1, and 1.15.1.	6.5	More Details
CVE-2021-28147	The team sync HTTP API in Grafana Enterprise 6.x before 6.7.6, 7.x before 7.3.10, and 7.4.x before 7.4.5 has an Incorrect Access Control issue. On Grafana instances using an external authentication service and having the EditorsCanAdmin feature enabled, this vulnerability allows any authenticated user to add external groups to any existing team. This can be used to grant a user team permissions that the user isn't supposed to have.	6.5	More Details
CVE-2021-21623	An incorrect permission check in Jenkins Matrix Authorization Strategy Plugin 2.6.5 and earlier allows attackers with Item/Read permission on nested items to access them, even if they lack Item/Read permission for parent folders.	6.5	More Details
CVE-2020-9212	There is a vulnerability in some version of USG9500 that the device improperly handles the information when a user logs in to device. The attacker can exploit the vulnerability to perform some operation and can get information and cause information leak.	6.5	More Details
CVE-2021-21390	MinIO is an open-source high performance object storage service and it is API compatible with Amazon S3 cloud storage service. In MinIO before version RELEASE.2021-03-17T02-33-02Z, there is a vulnerability which enables MITM modification of request bodies that are meant to have integrity guaranteed by chunk signatures. In a PUT request using aws-chunked encoding, MinIO ordinarily verifies signatures at the end of a chunk. This check can be skipped if the client sends a false chunk size that is much greater than the actual data sent: the server accepts and completes the request without ever reaching the end of the chunk + thereby without ever checking the chunk signature. This is fixed in version RELEASE.2021-03-17T02-33-02Z. As a workaround one can avoid using "aws-chunked" encoding-based chunk signature upload requests instead use TLS. MinIO SDKs automatically disable chunked encoding signature when the server endpoint is configured with TLS.	6.5	More Details
CVE-2021-20624	Improper access control vulnerability in Scheduler of Cybozu Office 10.0.0 to 10.8.4 allows an authenticated attacker to bypass access restriction and alter the data of Scheduler via unspecified vectors.	6.5	More Details
CVE-2021-20631	Improper input validation vulnerability in Custom App of Cybozu Office 10.0.0 to 10.8.4 allows authenticated attacker to alter the data of Custom App via unspecified vectors.	6.5	More Details
CVE-2021-20626	Improper access control vulnerability in Workflow of Cybozu Office 10.0.0 to 10.8.4 allows authenticated attackers to bypass access restriction and alter the data of Workflow via unspecified vectors.	6.5	More Details
CVE-2020-11230	Potential arbitrary memory corruption when the qseecom driver updates ion physical addresses in the buffer as it exposes a physical address to user land in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	6.4	More Details
CVE-2020-11220	While processing storage SCM commands there is a time of check or time of use window where a pointer used could be invalid at a specific time while executing the storage SCM call in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	6.4	More Details
CVE-2021-21376	OMERO.web is open source Django-based software for managing microscopy imaging. OMERO.web before version 5.9.0 loads various information about the current user such as their id, name and the groups they are in, and these are available on the main webclient pages. This represents an information exposure vulnerability. Some additional information being loaded is not used by the webclient and is being removed in this release. This is fixed in version 5.9.0.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10225	A flaw was found in atomic-openshift of openshift-4.2 where the basic-user RABC role in OpenShift Container Platform doesn't sufficiently protect the GlusterFS StorageClass against leaking of the restuserkey. An attacker with basic-user permissions is able to obtain the value of restuserkey, and use it to authenticate to the GlusterFS REST service, gaining access to read, and modify files.	6.3	More Details
CVE-2021-21384	shescape is a simple shell escape package for JavaScript. In shescape before version 1.1.3, anyone using _Shescape_ to defend against shell injection may still be vulnerable against shell injection if the attacker manages to insert a into the payload. For an example see the referenced GitHub Security Advisory. The problem has been patched in version 1.1.3. No further changes are required.	6.3	More Details
CVE-2021-28126	index.jsp in TranzWare e-Commerce Payment Gateway (TWEC PG) before 3.1.27.5 had a Stored cross-site scripting (XSS) vulnerability	6.1	More Details
CVE-2021-27519	A cross-site scripting (XSS) issue in FUDForum 3.1.0 allows remote attackers to inject JavaScript via index.php in the "srch" parameter.	6.1	More Details
CVE-2021-27520	A cross-site scripting (XSS) issue in FUDForum 3.1.0 allows remote attackers to inject JavaScript via index.php in the "author" parameter.	6.1	More Details
CVE-2021-21349	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	6.1	More Details
CVE-2021-27436	WebAccess/SCADA Versions 9.0 and prior is vulnerable to cross-site scripting, which may allow an attacker to send malicious JavaScript code to an unsuspecting user, which could result in hijacking of the user’s cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser actions.	6.1	More Details
CVE-2021-21346	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	6.1	More Details
CVE-2019-14830	A vulnerability was found in Moodle 3.7 to 3.7.1, 3.6 to 3.6.5, 3.5 to 3.5.7 and earlier unsupported versions, where the mobile launch endpoint contained an open redirect in some circumstances, which could result in a user's mobile access token being exposed. (Note: This does not affect sites with a forced URL scheme configured, mobile service disabled, or where the mobile app login method is "via the app").	6.1	More Details
CVE-2021-27309	Clansphere CMS 2011.4 allows unauthenticated reflected XSS via "module" parameter.	6.1	More Details
CVE-2019-14831	A vulnerability was found in Moodle 3.7 to 3.7.1, 3.6 to 3.6.5, 3.5 to 3.5.7 and earlier unsupported versions, where forum subscribe link contained an open redirect if forced subscription mode was enabled. If a forum's subscription mode was set to "forced subscription", the forum's subscribe link contained an open redirect.	6.1	More Details
CVE-2021-25277	FTAPI 4.0 - 4.10 allows XSS via a crafted filename to the alternative text hover box in the file submission component.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20628	Cross-site scripting vulnerability in Address Book of Cybozu Office 10.0.0 to 10.8.4 allows remote attackers to inject an arbitrary script via unspecified vectors. Note that this vulnerability occurs only when using Mozilla Firefox.	6.1	More Details
CVE-2020-6578	Zen Cart 1.5.6d allows reflected XSS via the main_page parameter to includes/templates/template_default/common/tpl_main_page.php or includes/templates/responsive_classic/common/tpl_main_page.php.	6.1	More Details
CVE-2021-28109	TranzWare (POI) FIMI before 4.2.20.4.2 allows login_tw.php reflected Cross-Site Scripting (XSS).	6.1	More Details
CVE-2021-20629	Cross-site scripting vulnerability in E-mail of Cybozu Office 10.0.0 to 10.8.4 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-20627	Cross-site scripting vulnerability in Address Book of Cybozu Office 10.0.0 to 10.8.4 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-21347	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	6.1	More Details
CVE-2021-25922	In OpenEMR, versions 4.2.0 to 6.0.0 are vulnerable to Reflected Cross-Site-Scripting (XSS) due to user input not being validated properly. An attacker could trick a user to click on a malicious url and execute malicious code.	6.1	More Details
CVE-2021-28957	An XSS vulnerability was discovered in python-lxml's clean module versions before 4.6.3. When disabling the safe_attrs_only and forms arguments, the Cleaner class does not remove the formaction attribute allowing for JS to bypass the sanitizer. A remote attacker could exploit this flaw to run arbitrary JS code on users who interact with incorrectly sanitized HTML. This issue is patched in lxml 4.6.3.	6.1	More Details
CVE-2021-28160	Wireless-N WiFi Repeater REV 1.0 (28.08.06.1) suffers from a reflected XSS vulnerability due to unsanitized SSID value when the latter is displayed in the /repeater.html page ("Repeater Wizard" homepage section).	6.1	More Details
CVE-2021-24124	Unvalidated input and lack of output encoding in the WP Shieldon WordPress plugin, version 1.6.3 and below, leads to Unauthenticated Reflected Cross-Site Scripting (XSS) when the CAPTCHA page is shown could lead to privileged escalation.	6.1	More Details
CVE-2020-4882	IBM Planning Analytics 2.0 could be vulnerable to a Server-Side Request Forgery (SSRF) attack by constucting URLs from user-controlled data . This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 190852.	6.1	More Details
CVE-2021-27310	Clansphere CMS 2011.4 allows unauthenticated reflected XSS via "language" parameter.	6.1	More Details
CVE-2019-18233	In Advantech Spectre RT Industrial Routers ERT351 5.1.3 and prior, the affected product does not neutralize special characters in the error response, allowing attackers to use a reflected XSS attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24135	Unvalidated input and lack of output encoding in the WP Customer Reviews WordPress plugin, versions before 3.4.3, lead to multiple Stored Cross-Site Scripting vulnerabilities allowing remote attackers to inject arbitrary JavaScript code or HTML.	6.1	More Details
CVE-2021-28796	Increments Qiita::Markdown before 0.33.0 allows XSS in transformers.	6.1	More Details
CVE-2020-27171	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c has an off-by-one error (with a resultant integer underflow) affecting out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-10d2bb2e6b1d.	6.0	More Details
CVE-2021-3416	A potential stack overflow via infinite loop issue was found in various NIC emulators of QEMU in versions up to and including 5.2.0. The issue occurs in loopback mode of a NIC wherein reentrant DMA checks get bypassed. A guest user/process may use this flaw to consume CPU cycles or crash the QEMU process on the host resulting in DoS scenario.	6.0	More Details
CVE-2021-21339	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 6.2.57, 7.6.51, 8.7.40, 9.5.25, 10.4.14, 11.1.1 user session identifiers were stored in cleartext - without processing of additional cryptographic hashing algorithms. This vulnerability cannot be exploited directly and occurs in combination with a chained attack - like for instance SQL injection in any other component of the system. This is fixed in versions 6.2.57, 7.6.51, 8.7.40, 9.5.25, 10.4.14, 11.1.1.	5.9	More Details
CVE-2021-21359	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 9.5.25, 10.4.14, 11.1.1 requesting invalid or non-existing resources via HTTP triggers the page error handler which again could retrieve content to be shown as error message from another page. This leads to a scenario in which the application is calling itself recursively - amplifying the impact of the initial attack until the limits of the web server are exceeded. This is fixed in versions 9.5.25, 10.4.14, 11.1.1.	5.9	More Details
CVE-2021-21345	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker who has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.8	More Details
CVE-2021-27908	In all versions prior to Mautic 3.3.2, secret parameters such as database credentials could be exposed publicly by an authorized admin user through leveraging Symfony parameter syntax in any of the free text fields in Mautic’s configuration that are used in publicly facing parts of the application.	5.8	More Details
CVE-2021-3409	The patch for CVE-2020-17380/CVE-2020-25085 was found to be ineffective, thus making QEMU vulnerable to the out-of-bounds read/write access issues previously found in the SDHCI controller emulation code. This flaw allows a malicious privileged guest to crash the QEMU process on the host, resulting in a denial of service or potential code execution. QEMU up to (including) 5.2.0 is affected by this.	5.7	More Details
CVE-2020-11199	HLOS to access EL3 stack canary by just mapping imem region due to Improper access control and can lead to information exposure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	5.5	More Details
CVE-2021-27906	A carefully crafted PDF file can trigger an OutOfMemory-Exception while loading the file. This issue affects Apache PDFBox version 2.0.22 and prior 2.0.x versions.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28971	In intel_pmu_drain_pebs_nhm in arch/x86/events/intel/ds.c in the Linux kernel through 5.11.8 on some Haswell CPUs, userspace applications (such as perf-fuzzer) can cause a system crash because the PEBS status in a PEBS record is mishandled, aka CID-d88d05a9e0b6.	5.5	More Details
CVE-2021-24138	Unvalidated input in the AdRotate WordPress plugin, versions before 5.8.4, leads to Authenticated SQL injection via param "id". This requires an admin privileged user.	5.5	More Details
CVE-2020-35456	The Taidii Diibear Android application 2.4.0 and all its derivatives allow attackers to view private chat messages and media files via logcat because of excessive logging.	5.5	More Details
CVE-2021-28950	An issue was discovered in fs/fuse/fuse_i.h in the Linux kernel before 5.11.8. A "stall on CPU" can occur because a retry loop continually finds the same bad inode, aka CID-775c5033a0d1.	5.5	More Details
CVE-2021-28951	An issue was discovered in fs/io_uring.c in the Linux kernel through 5.11.8. It allows attackers to cause a denial of service (deadlock) because exit may be waiting to park a SQPOLL thread, but concurrently that SQPOLL thread is waiting for a signal to start, aka CID-3ebba796fa25.	5.5	More Details
CVE-2021-20227	A flaw was found in SQLite's SELECT query functionality (src/select.c). This flaw allows an attacker who is capable of running SQL queries locally on the SQLite database to cause a denial of service or possible code execution by triggering a use-after-free. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2021-27807	A carefully crafted PDF file can trigger an infinite loop while loading the file. This issue affects Apache PDFBox version 2.0.22 and prior 2.0.x versions.	5.5	More Details
CVE-2020-11221	Usage of syscall by non-secure entity can allow extraction of secure QTEE diagnostic information in clear text form due to insufficient checks in the syscall handler and leads to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	5.5	More Details
CVE-2021-28650	autoar-extractor.c in GNOME gnome-autoar before 0.3.1, as used by GNOME Shell, Nautilus, and other software, allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink in certain complex situations. NOTE: this issue exists because of an incomplete fix for CVE-2020-36241.	5.5	More Details
CVE-2020-11186	Modem will enter into busy mode in an infinite loop while parsing histogram dimension due to improper validation of input received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	5.5	More Details
CVE-2021-27506	The ClamAV Engine (version 0.103.1 and below) component embedded in Storsmshield Network Security (SNS) is subject to DoS in case of parsing of malformed png files. This affect Netasq versions 9.1.0 to 9.1.11 and SNS versions 1.0.0 to 4.2.0. This issue is fixed in SNS 3.7.19, 3.11.7 and 4.2.1.	5.5	More Details
CVE-2021-20219	A denial of service vulnerability was found in n_tty_receive_char_special in drivers/tty/n_tty.c of the Linux kernel. In this flaw a local attacker with a normal user privilege could delay the loop (due to a changing ldata->read_head, and a missing sanity check) and cause a threat to the system availability.	5.5	More Details
CVE-2021-28100	Priam uses File.createTempFile, which gives the permissions on that file -rw-r--r--. An attacker with read access to the local filesystem can read anything written there by the Priam process.	5.5	More Details
CVE-2021-24126	Unvalidated input and lack of output encoding in the Envira Gallery Lite WordPress plugin, versions before 1.8.3.3, did not properly sanitise the images metadata (namely title) before outputting them in the generated gallery, which could lead to privilege escalation.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3327	Ovation Dynamic Content 1.10.1 for Elementor allows XSS via the post_title parameter.	5.4	More Details
CVE-2021-24127	Unvalidated input and lack of output encoding in the ThirstyAffiliates Affiliate Link Manager WordPress plugin, versions before 3.9.3, was vulnerable to authenticated Stored Cross-Site Scripting (XSS), which could lead to privilege escalation.	5.4	More Details
CVE-2021-24128	Unvalidated input and lack of output encoding in the Team Members WordPress plugin, versions before 5.0.4, lead to Cross-site scripting vulnerabilities allowing medium-privileged authenticated attacker (contributor+) to inject arbitrary web script or HTML via the 'Description/biography' of a member.	5.4	More Details
CVE-2021-24129	Unvalidated input and lack of output encoding in the Themify Portfolio Post WordPress plugin, versions before 1.1.6, lead to Stored Cross-Site Scripting (XSS) vulnerabilities allowing low-privileged users (Contributor+) to inject arbitrary JavaScript code or HTML in posts where the Themify Custom Panel is embedded, which could lead to privilege escalation.	5.4	More Details
CVE-2021-21358	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 10.4.14, 11.1.1 it has been discovered that the Form Designer backend module of the Form Framework is vulnerable to cross-site scripting. A valid backend user account with access to the form module is needed to exploit this vulnerability. This is fixed in versions 10.4.14, 11.1.1.	5.4	More Details
CVE-2021-24136	Unvalidated input and lack of output encoding in the Testimonials Widget WordPress plugin, versions before 4.0.0, lead to multiple Cross-Site Scripting vulnerabilities, allowing remote attackers to inject arbitrary JavaScript code or HTML via the below parameters: - Author - Job Title - Location - Company - Email - URL	5.4	More Details
CVE-2021-21340	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 10.4.14, 11.1.1 it has been discovered that database fields used as _descriptionColumn_ are vulnerable to cross-site scripting when their content gets previewed. A valid backend user account is needed to exploit this vulnerability. This is fixed in versions 10.4.14, 11.1.1 .	5.4	More Details
CVE-2021-24147	Unvalidated input and lack of output encoding in the Modern Events Calendar Lite WordPress plugin, versions before 5.16.5, did not sanitise the mic_comment field (Notes on time) when adding/editing an event, allowing users with privilege as low as author to add events with a Cross-Site Scripting payload in them, which will be triggered in the frontend when viewing the event.	5.4	More Details
CVE-2021-21370	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 7.6.51, 8.7.40, 9.5.25, 10.4.14, 11.1.1 it has been discovered that content elements of type _menu_ are vulnerable to cross-site scripting when their referenced items get previewed in the page module. A valid backend user account is needed to exploit this vulnerability. This is fixed in versions 7.6.51, 8.7.40, 9.5.25, 10.4.14, 11.1.1.	5.4	More Details
CVE-2021-28968	An issue was discovered in PunBB before 1.4.6. An XSS vulnerability in the [email] BBcode tag allows (with authentication) injecting arbitrary JavaScript into any forum message.	5.4	More Details
CVE-2021-28145	Concrete CMS (formerly concrete5) before 8.5.5 allows remote authenticated users to conduct XSS attacks via a crafted survey block. This requires at least Editor privileges.	5.4	More Details
CVE-2021-21351	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17457	Fujitsu ServerView Suite iRMC before 9.62F allows XSS. An authenticated attacker can store an XSS payload in the PSCU_FILE_INIT field of a Save Configuration XML document. The payload is triggered in the HTTP error response pages.	5.4	More Details
CVE-2021-25921	In OpenEMR, versions 2.7.3-rc1 to 6.0.0 are vulnerable to Stored Cross-Site-Scripting (XSS) due to user input not being validated properly in the `Allergies` section. An attacker could lure an admin to enter a malicious payload and by that initiate the exploit.	5.4	More Details
CVE-2021-21343	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability where the processed stream at unmarshalling time contains type information to recreate the formerly written objects. XStream creates therefore new instances based on these type information. An attacker can manipulate the processed input stream and replace or inject objects, that result in the deletion of a file on the local host. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.3	More Details
CVE-2020-28501	This affects the package es6-crawler-detect before 3.1.3. No limitation of user agent string length supplied to regex operators.	5.3	More Details
CVE-2021-28963	Shibboleth Service Provider before 3.2.1 allows content injection because template generation uses attacker-controlled parameters.	5.3	More Details
CVE-2021-26069	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to download temporary files and enumerate project keys via an Information Disclosure vulnerability in the /rest/api/1.0/issues/{id}/ActionsAndOperations API endpoint. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.15.0.	5.3	More Details
CVE-2021-21342	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability where the processed stream at unmarshalling time contains type information to recreate the formerly written objects. XStream creates therefore new instances based on these type information. An attacker can manipulate the processed input stream and replace or inject objects, that result in a server-side forgery request. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.3	More Details
CVE-2021-28681	Pion WebRTC before 3.0.15 didn't properly tear down the DTLS Connection when certificate verification failed. The PeerConnectionState was set to failed, but a user could ignore that and continue to use the PeerConnection.)A WebRTC implementation shouldn't allow the user to continue if verification has failed.)	5.3	More Details
CVE-2020-36144	Redash 8.0.0 is affected by LDAP Injection. There is an information leak through the crafting of special queries, escaping the provided template since the username included in the search filter lacks sanitization.	5.3	More Details
CVE-2020-4635	IBM Resilient SOAR 40 and earlier could disclose sensitive information by allowing a user to enumerate usernames.	5.3	More Details
CVE-2021-21344	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25764	In JetBrains PhpStorm before 2020.3, source code could be added to debug logs.	5.3	More Details
CVE-2021-22321	There is a use-after-free vulnerability in a Huawei product. A module cannot deal with specific operations in special scenarios. Attackers can exploit this vulnerability by performing malicious operations. This can cause memory use-after-free, compromising normal service. Affected product include some versions of NIP6300, NIP6600, NIP6800, S1700, S2700, S5700, S6700 , S7700, S9700, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	5.3	More Details
CVE-2021-28090	Tor before 0.4.5.7 allows a remote attacker to cause Tor directory authorities to exit with an assertion failure, aka TROVE-2021-002.	5.3	More Details
CVE-2021-21350	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to execute arbitrary code only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.3	More Details
CVE-2021-23362	The package hosted-git-info before 3.0.8 are vulnerable to Regular Expression Denial of Service (ReDoS) via regular expression shortcutMatch in the fromUrl function in index.js. The affected regular expression exhibits polynomial worst-case time complexity.	5.3	More Details
CVE-2021-21348	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to occupy a thread that consumes maximum CPU time and will never return. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.	5.3	More Details
CVE-2021-27656	A vulnerability in exacqVision Web Service 20.12.2.0 and prior could allow an unauthenticated attacker to view system-level information about the exacqVision Web Service and the operating system.	5.3	More Details
CVE-2021-27527	A cross-site scripting (XSS) vulnerability in DynPG version 4.9.2 allows remote attackers to inject JavaScript via the "valueID" parameter.	4.8	More Details
CVE-2021-24134	Unvalidated input and lack of output encoding in the Constant Contact Forms WordPress plugin, versions before 1.8.8, lead to multiple Stored Cross-Site Scripting vulnerabilities, which allowed high-privileged user (Editor+) to inject arbitrary JavaScript code or HTML in posts where the malicious form is embed.	4.8	More Details
CVE-2021-27969	Dolphin CMS 7.4.2 is vulnerable to stored XSS via the Page Builder "width" parameter.	4.8	More Details
CVE-2021-27528	A cross-site scripting (XSS) vulnerability in DynPG version 4.9.2 allows remote attackers to inject JavaScript via the "refID" parameter.	4.8	More Details
CVE-2021-25918	In OpenEMR, versions 5.0.2 to 6.0.0 are vulnerable to Stored Cross-Site-Scripting (XSS) due to user input not being validated properly and rendered in the TOTP Authentication method page. A highly privileged attacker could inject arbitrary code into input fields when creating a new user.	4.8	More Details
CVE-2021-27529	A cross-site scripting (XSS) vulnerability in DynPG version 4.9.2 allows remote attackers to inject JavaScript via the "limit" parameter.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27530	A cross-site scripting (XSS) vulnerability in DynPG version 4.9.2 allow remote attacker to inject javascript via URI in /index.php.	4.8	More Details
CVE-2021-27526	A cross-site scripting (XSS) vulnerability in DynPG version 4.9.2 allows remote attackers to inject JavaScript via the "page" parameter.	4.8	More Details
CVE-2021-27531	A cross-site scripting (XSS) vulnerability in DynPG version 4.9.2 allows remote attackers to inject JavaScript via the "query" parameter.	4.8	More Details
CVE-2021-25917	In OpenEMR, versions 5.0.2 to 6.0.0 are vulnerable to Stored Cross-Site-Scripting (XSS) due to user input not being validated properly and rendered in the U2F USB Device authentication method page. A highly privileged attacker could inject arbitrary code into input fields when creating a new user.	4.8	More Details
CVE-2021-25919	In OpenEMR, versions 5.0.2 to 6.0.0 are vulnerable to Stored Cross-Site-Scripting (XSS) due to user input not being validated properly. A highly privileged attacker could inject arbitrary code into input fields when creating a new user.	4.8	More Details
CVE-2021-28420	A cross-site scripting (XSS) issue in Seo Panel 4.8.0 allows remote attackers to inject JavaScript via alerts.php and the "from_time" parameter.	4.8	More Details
CVE-2021-28418	A cross-site scripting (XSS) issue in Seo Panel 4.8.0 allows remote attackers to inject JavaScript via settings.php and the "category" parameter.	4.8	More Details
CVE-2021-28417	A cross-site scripting (XSS) issue in Seo Panel 4.8.0 allows remote attackers to inject JavaScript via archive.php and the "search_name" parameter.	4.8	More Details
CVE-2021-27308	A cross-site scripting (XSS) vulnerability in the admin login panel in 4images version 1.8 allows remote attackers to inject JavaScript via the "redirect" parameter.	4.8	More Details
CVE-2021-25278	FTAPI 4.0 through 4.10 allows XSS via an SVG document to the Background Image upload feature in the Submit Box Template Editor.	4.8	More Details
CVE-2021-21377	OMERO.web is open source Django-based software for managing microscopy imaging. OMERO.web before version 5.9.0 supports redirection to a given URL after performing login or switching the group context. These URLs are not validated, allowing redirection to untrusted sites. OMERO.web 5.9.0 adds URL validation before redirecting. External URLs are not considered valid, unless specified in the omero.web.redirect_allowed_hosts setting.	4.8	More Details
CVE-2021-21338	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 6.2.57, 7.6.51, 8.7.40, 9.5.25, 10.4.14, 11.1.1 it has been discovered that Login Handling is susceptible to open redirection which allows attackers redirecting to arbitrary content, and conducting phishing attacks. No authentication is required in order to exploit this vulnerability. This is fixed in versions 6.2.57, 7.6.51, 8.7.40, 9.5.25, 10.4.14, 11.1.1.	4.7	More Details
CVE-2021-28964	A race condition was discovered in get_old_root in fs/btrfs/ctree.c in the Linux kernel through 5.11.8. It allows attackers to cause a denial of service (BUG) because of a lack of locking on an extent buffer before a cloning operation, aka CID-dbcc7d57bffc.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27170	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-f232326f6966. This affects pointer types that do not define a ptr_limit.	4.7	More Details
CVE-2021-28099	In Netflix OSS Hollow, since the Files.exists(parent) is run before creating the directories, an attacker can pre-create these directories with wide permissions. Additionally, since an insecure source of randomness is used, the file names to be created can be deterministically calculated.	4.4	More Details
CVE-2021-22310	There is an information leakage vulnerability in some huawei products. Due to the properly storage of specific information in the log file, the attacker can obtain the information when a user logs in to the device. Successful exploit may cause an information leak. Affected product versions include: NIP6300 versions V500R001C00,V500R001C20,V500R001C30;NIP6600 versions V500R001C00,V500R001C20,V500R001C30;Secospace USG6300 versions V500R001C00,V500R001C20,V500R001C30;Secospace USG6500 versions V500R001C00,V500R001C20,V500R001C30;Secospace USG6600 versions V500R001C00,V500R001C20,V500R001C30,V500R001C50,V500R001C60,V500R001C80;USG9500 versions V500R005C00,V500R005C10.	4.4	More Details
CVE-2021-20633	Improper access control vulnerability in Cabinet of Cybozu Office 10.0.0 to 10.8.4 allows authenticated attackers to bypass access restriction and obtain the date of Cabinet via unspecified vectors.	4.3	More Details
CVE-2021-20634	Improper access control vulnerability in Custom App of Cybozu Office 10.0.0 to 10.8.4 allows authenticated attackers to bypass access restriction and obtain the date of Custom App via unspecified vectors.	4.3	More Details
CVE-2019-14829	A vulnerability was found in Moodle affection 3.7 to 3.7.1, 3.6 to 3.6.5, 3.5 to 3.5.7 and earlier unsupported versions where activity creation capabilities were not correctly respected when selecting the activity to use for a course in single activity mode.	4.3	More Details
CVE-2021-21625	Jenkins CloudBees AWS Credentials Plugin 1.28 and earlier does not perform a permission check in a helper method for HTTP endpoints, allowing attackers with Overall/Read permission to enumerate credentials IDs of AWS credentials stored in Jenkins in some circumstances.	4.3	More Details
CVE-2021-21624	An incorrect permission check in Jenkins Role-based Authorization Strategy Plugin 3.1 and earlier allows attackers with Item/Read permission on nested items to access them, even if they lack Item/Read permission for parent folders.	4.3	More Details
CVE-2021-20625	Improper access control vulnerability in Bulletin Board of Cybozu Office 10.0.0 to 10.8.4 allows an authenticated attacker to bypass access restriction and alter the data of Bulletin Board via unspecified vectors.	4.3	More Details
CVE-2021-24133	Lack of CSRF checks in the ActiveCampaign WordPress plugin, versions before 8.0.2, on its Settings form, which could allow attacker to make a logged-in administrator change API Credentials to attacker's account.	4.3	More Details
CVE-2021-20676	M-System DL8 series (type A (DL8-A) versions prior to Ver3.0, type B (DL8-B) versions prior to Ver3.0, type C (DL8-C) versions prior to Ver3.0, type D (DL8-D) versions prior to Ver3.0, and type E (DL8-E) versions prior to Ver3.0) allows remote authenticated attackers to bypass access restriction and conduct prohibited operations via unspecified vectors.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28133	Zoom through 5.5.4 sometimes allows attackers to read private information on a participant's screen, even though the participant never attempted to share the private part of their screen. When a user shares a specific application window via the Share Screen functionality, other meeting participants can briefly see contents of other application windows that were explicitly not shared. The contents of these other windows can (for instance) be seen for a short period of time when they overlay the shared window and get into focus. (An attacker can, of course, use a separate screen-recorder application, unsupported by Zoom, to save all such contents for later replays and analysis.) Depending on the unintentionally shared data, this short exposure of screen contents may be a more or less severe security issue.	4.3	More Details
CVE-2021-26216	SeedDMS 5.1.x is affected by cross-site request forgery (CSRF) in out.EditFolder.php.	4.3	More Details
CVE-2019-14828	A vulnerability was found in Moodle affecting 3.7 to 3.7.1, 3.6 to 3.6.5, 3.5 to 3.5.7 and earlier unsupported versions, where users with the capability to create courses were assigned as a teacher in those courses, regardless of whether they had the capability to be automatically assigned that role.	4.3	More Details
CVE-2021-20632	Improper access control vulnerability in Bulletin Board of Cybozu Office 10.0.0 to 10.8.4 allows authenticated attackers to bypass access restriction and obtain the data of Bulletin Board via unspecified vectors.	4.3	More Details
CVE-2021-20630	Improper access control vulnerability in Phone Messages of Cybozu Office 10.0.0 to 10.8.4 allows authenticated attackers to bypass access restriction and obtain the data of Phone Messages via unspecified vectors.	4.3	More Details
CVE-2021-26215	SeedDMS 5.1.x is affected by cross-site request forgery (CSRF) in out.EditDocument.php.	4.3	More Details
CVE-2021-21626	Jenkins Warnings Next Generation Plugin 8.4.4 and earlier does not perform a permission check in methods implementing form validation, allowing attackers with Item/Read permission but without Item/Workspace or Item/Configure permission to check whether attacker-specified file patterns match workspace contents.	4.3	More Details
CVE-2019-3867	A vulnerability was found in the Quay web application. Sessions in the Quay web application never expire. An attacker, able to gain access to a session, could use it to control or delete a user's container repository. Red Hat Quay 2 and 3 are vulnerable to this issue.	4.1	More Details
CVE-2019-14850	A denial of service vulnerability was discovered in nbdkit 1.12.7, 1.14.1 and 1.15.1. An attacker could connect to the nbdkit service and cause it to perform a large amount of work in initializing backend plugins, by simply opening a connection to the service. This vulnerability could cause resource consumption and degradation of service in nbdkit, depending on the plugins configured on the server-side.	3.7	More Details
CVE-2021-21437	Agents are able to see linked Config Items without permissions, which are defined in General Catalog. This issue affects: OTRSCIsInCustomerFrontend 7.0.15 and prior versions, ITSMConfigurationManagement 7.0.24 and prior versions	3.5	More Details
CVE-2021-21438	Agents are able to see linked FAQ articles without permissions (defined in FAQ Category). This issue affects: FAQ version 6.0.29 and prior versions, OTRS version 7.0.24 and prior versions.	3.5	More Details
CVE-2021-27593	When a user opens manipulated Graphics Interchange Format (.GIF) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27594	When a user opens manipulated Windows Bitmap (.BMP) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details
CVE-2021-27595	When a user opens manipulated Portable Document Format (.PDF) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details
CVE-2021-27596	When a user opens manipulated Autodesk 3D Studio for MS-DOS (.3DS) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details
CVE-2021-3392	A use-after-free flaw was found in the MegaRAID emulator of QEMU. This issue occurs while processing SCSI I/O requests in the case of an error mptsas_free_request() that does not dequeue the request object 'req' from a pending requests queue. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. Versions between 2.10.0 and 5.2.0 are potentially affected.	3.2	More Details
CVE-2020-13606	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-15282	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-13608	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-13604	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-13607	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-13610	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-13609	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-13612	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-13611	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-15281	Rejected reason: Unused CVE for 2020	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13605	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-14358	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-2021-23361	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-2020-15759	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2019-14848	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-2020-15751	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15752	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15753	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15754	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15755	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15756	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15757	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15758	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15760	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2019-14908	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 Number	Description	Base Score	Reference
CVE-2020-15761	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15762	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15763	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15764	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15765	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15766	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-8106	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-8111	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2021-20200	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-2019-14903	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-2020-15750	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15285	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15728	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15286	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15287	Rejected reason: Unused CVE for 2020	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15288	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15289	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15290	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15291	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15295	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15296	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15298	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15736	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15749	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15737	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15738	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15740	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15741	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15743	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15745	Rejected reason: Unused CVE for 2020	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15746	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15747	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2020-15748	Rejected reason: Unused CVE for 2020	N/A	More Details
CVE-2019-10151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details