SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 June 2021

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-26472	In VembuBDR before 4.2.0.1 and VembuOffsiteDR before 4.2.0.1 installed on Windows, the http API located at /consumerweb/secure/download.php. Using this command argument an unauthenticated attacker can execute arbitrary OS commands with SYSTEM privileges.	10.0	More Details
CVE-2021-32671	Flarum is a forum software for building communities. Flarum's translation system allowed for string inputs to be converted into HTML DOM nodes when rendered. This change was made after v0.1.0-beta.16 (our last beta before v1.0.0) and was not noticed or documented. This allowed for any user to type malicious HTML markup within certain user input fields and have this execute on client browsers. The example which led to the discovery of this vulnerability was in the forum search box. Entering faux-malicious HTML markup, such as <script>alert('test')</script> resulted in an alert box appearing on the forum. This attack could also be modified to perform AJAX requests on behalf of a user, possibly deleting discussions, modifying their settings or profile, or even modifying settings on the Admin panel if the attack was targetted towards a privileged user. All Flarum communities that run flarum v1.0.0 or v1.0.1 are impacted. The vulnerability has been fixed and published as flarum/core v1.0.2. All communities running Flarum v1.0 have to upgrade as soon as possible to v1.0.2.	10.0	More Details
CVE-2021-29089	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in thumbnail component in Synology Photo Station before 6.8.14-3500 allows remote attackers users to execute arbitrary SQL commands via unspecified vectors.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33806	The BDew BdLib library before 1.16.1.7 for Minecraft allows remote code execution because it deserializes untrusted data in ObjectInputStream.readObject as part of its use of Java serialization.	9.8	More Details
CVE-2021-26473	In VembuBDR before 4.2.0.1 and VembuOffsiteDR before 4.2.0.1 the http API located at /sgwebservice_o.php action logFilePath allows an attacker to write arbitrary files in the context of the web server process. These files can then be executed remotely by calling the file via the web server.	9.8	More Details
CVE-2021-26471	In VembuBDR before 4.2.0.1 and VembuOffsiteDR before 4.2.0.1, the http API located at /sgwebservice_o.php accepts a command argument. Using this command argument an unauthenticated attacker can execute arbitrary shell commands.	9.8	More Details
CVE-2021-28293	Seceon aiSIEM before 6.3.2 (build 585) is prone to an unauthenticated account takeover vulnerability in the Forgot Password feature. The lack of correct configuration leads to recovery of the password reset link generated via the password reset functionality, and thus an unauthenticated attacker can set an arbitrary password for any user.	9.8	More Details
CVE-2021-20699	Sharp NEC Displays ((UN462A R1.300 and prior to it, UN462VA R1.300 and prior to it, UN492S R1.300 and prior to it, UN492VS R1.300 and prior to it, UN552A R1.300 and prior to it, UN552S R1.300 and prior to it, UN552VS R1.300 and prior to it, UN552 R1.300 and prior to it, UN552V R1.300 and prior to it, UX552S R1.300 and prior to it, UX552 R1.300 and prior to it, V864Q R2.000 and prior to it, C861Q R2.000 and prior to it, P754Q R2.000 and prior to it, V754Q R2.000 and prior to it, C751Q R2.000 and prior to it, V984Q R2.000 and prior to it, C981Q R2.000 and prior to it, P654Q R2.000 and prior to it, V654Q R2.000 and prior to it, C651Q R2.000 and prior to it, V554Q R2.000 and prior to it, P404 R3.200 and prior to it, P484 R3.200 and prior to it, P554 R3.200 and prior to it, V404 R3.200 and prior to it, V484 R3.200 and prior to it, V554 R3.200 and prior to it, V404-T R3.200 and prior to it, V484-T R3.200 and prior to it, V554-T R3.200 and prior to it, C501 R2.000 and prior to it, C551 R2.000 and prior to it, C431 R2.000 and prior to it) allows an attacker a buffer overflow and to execute remote code by sending long parameters that contains specific characters in http request.	9.8	More Details
CVE-2021-20698	Sharp NEC Displays (UN462A R1.300 and prior to it, UN462VA R1.300 and prior to it, UN492S R1.300 and prior to it, UN492VS R1.300 and prior to it, UN552A R1.300 and prior to it, UN552S R1.300 and prior to it, UN552VS R1.300 and prior to it, UN552 R1.300 and prior to it, UN552V R1.300 and prior to it, UX552S R1.300 and prior to it, UX552 R1.300 and prior to it, V864Q R2.000 and prior to it, C861Q R2.000 and prior to it, P754Q R2.000 and prior to it, V754Q R2.000 and prior to it, C751Q R2.000 and prior to it, V984Q R2.000 and prior to it, C981Q R2.000 and prior to it, P654Q R2.000 and prior to it, V654Q R2.000 and prior to it, C651Q R2.000 and prior to it, V554Q R2.000 and prior to it, P404 R3.200 and prior to it, P484 R3.200 and prior to it, P554 R3.200 and prior to it, V404 R3.200 and prior to it, V484 R3.200 and prior to it, V554 R3.200 and prior to it, V404-T R3.200 and prior to it, V484-T R3.200 and prior to it, V554-T R3.200 and prior to it, C501 R2.000 and prior to it, C551 R2.000 and prior to it, C431 R2.000 and prior to it) allows an attacker to obtain root privileges and execute remote code by sending unintended parameters that contain specific characters in http request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20005	NGINX before 1.13.6 has a buffer overflow for years that exceed four digits, as demonstrated by a file with a modification date in 1969 that causes an integer overflow (or a false modification date far in the future), when encountered by the autoindex module.	9.8	More Details
CVE-2021-32198	EmTec ZOC through 8.02.4 allows remote servers to cause a denial of service (Windows GUI hang) by telling the ZOC window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. In other words, it does not implement a usleep or similar delay upon processing a title change.	9.8	More Details
CVE-2021-31251	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated.	9.8	More Details
CVE-2021-30475	aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buffer overflow.	9.8	More Details
CVE-2021-25947	Prototype pollution vulnerability in 'nestie' versions 0.0.0 through 1.0.0 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-22333	There is an Improper Validation of Array Index vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause code to execute, thus obtaining system permissions.	9.8	More Details
CVE-2020-35442	FDCMS (also known as Fangfa Content Management System) 4.0 allows remote attackers to get a webshell in the background via Front/lib/Action/FindexAction.class.php.	9.8	More Details
CVE-2020-35441	FDCMS (aka Fangfa Content Management System) 4.0 contains a front-end SQL injection via Admin/Lib/Action/FloginAction.class.php.	9.8	More Details
CVE-2021-30474	aom_dsp/grain_table.c in libaom in AOMedia before 2021-03-30 has a use-after-free.	9.8	More Details
CVE-2021-31921	Istio before 1.8.6 and 1.9.x before 1.9.5 contains a remotely exploitable vulnerability where an external client can access unexpected services in the cluster, bypassing authorization checks, when a gateway is configured with AUTO_PASSTHROUGH routing configuration.	9.8	More Details
CVE-2009-0948	Multiple buffer overflows in the (1) cdf_read_sat, (2) cdf_read_long_sector_chain, and (3) cdf_read_ssat function in file before 5.02.	9.8	More Details
CVE-2009-0947	Multiple integer overflows in the (1) cdf_read_property_info and (2) cdf_read_sat functions in file before 5.02.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26707	The merge-deep library before 3.0.3 for Node.js can be tricked into overwriting properties of Object.prototype or adding new properties to it. These properties are then inherited by every object in the program, thus facilitating prototype-pollution attacks against applications using this library.	9.8	More Details
CVE-2021-3538	A flaw was found in github.com/satori/go.uuid in versions from commit 0ef6afb2f6cdd6cdaeee3885a95099c63f18fc8c to d91630c8510268e75203009fe7daf2b8e1d60c45. Due to insecure randomness in the g.rand.Read function the generated UUIDs are predictable for an attacker.	9.8	More Details
CVE-2021-3520	There's a flaw in lz4. An attacker who submits a crafted file to an application linked with lz4 may be able to trigger an integer overflow, leading to calling of memmove() on a negative size argument, causing an out-of-bounds write and/or a crash. The greatest impact of this flaw is to availability, with some potential impact to confidentiality and integrity as well.	9.8	More Details
CVE-2021-23894	Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote unauthenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server.	9.6	More Details
CVE-2021-31962	Kerberos AppContainer Security Feature Bypass Vulnerability	9.4	More Details
CVE-2021-25288	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_gray_i.	9.1	More Details
CVE-2021-25287	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_graya_la.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29504	WP-CLI is the command-line interface for WordPress. An improper error handling in HTTPS requests management in WP-CLI version 0.12.0 and later allows remote attackers able to intercept the communication to remotely disable the certificate verification on WP-CLI side, gaining full control over the communication content, including the ability to impersonate update servers and push malicious updates towards WordPress instances controlled by the vulnerable WP-CLI agent, or push malicious updates toward WP-CLI itself. The vulnerability stems from the fact that the default behavior of `WP_CLI\Utils\http_request()` when encountering a TLS handshake error is to disable certificate validation and retry the same request. The default behavior has been changed with version 2.5.0 of WP-CLI and the `wp-cli/wp-cli` framework (via https://github.com/wp-cli/wp-cli/pull/5523) so that the `WP_CLI\Utils\http_request()` method accepts an `$insecure` option that is `false` by default and consequently that a TLS handshake failure is a hard error by default. This new default is a breaking change and ripples through to all consumers of `WP_CLI\Utils\http_request()`, including those in separate WP-CLI bundled or third-party packages. https://github.com/wp-cli/wp-cli/pull/5523 has also added an `--insecure` flag to the `cli update` command to counter this breaking change. There is no direct workaround for the default insecure behavior of `wp-cli/wp-cli` versions before 2.5.0. The workaround for dealing with the breaking change in the commands directly affected by the new secure default behavior is to add the `--insecure` flag to manually opt-in to the previous insecure behavior.	9.1	More Details
CVE-2021-23895	Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-30529	Use after free in Bookmarks in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-36141	BloofoxCMS 0.5.2.1 allows Unrestricted File Upload vulnerability via bypass MIME Type validation by inserting 'image/jpeg' within the 'Content-Type' header.	8.8	More Details
CVE-2021-24337	The id GET parameter of one of the Video Embed WordPress plugin through 1.0's page (available via forced browsing) is not sanitised, validated or escaped before being used in a SQL statement, allowing low privilege users, such as subscribers, to perform SQL injection.	8.8	More Details
CVE-2021-22213	A cross-site leak vulnerability in the OAuth flow of all versions of GitLab CE/EE since 7.10 allowed an attacker to leak an OAuth access token by getting the victim to visit a malicious page with Safari	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23169	A heap-buffer overflow was found in the copyIntoFrameBuffer function of OpenEXR in versions before 3.0.1. An attacker could use this flaw to execute arbitrary code with the permissions of the user running the application compiled against OpenEXR.	8.8	More Details
CVE-2021-30528	Use after free in WebAuthentication in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker who had compromised the renderer process of a user who had saved a credit card in their Google account to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-20517	IBM WebSphere Application Server Network Deployment 8.5 and 9.0 could allow a remote authenticated attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to read and delete arbitrary files on the system. IBM X-Force ID: 198435.	8.8	More Details
CVE-2020-26516	A CSRF issue was discovered in Intland codeBeamer ALM 10.x through 10.1.SP4. Requests sent to the server that trigger actions do not contain a CSRF token and can therefore be entirely predicted allowing attackers to cause the victim's browser to execute undesired actions in the web application through crafted requests.	8.8	More Details
CVE-2020-24870	Libraw before 0.20.1 has a stack buffer overflow via LibRaw::identify_process_dng_fields in identify.cpp.	8.8	More Details
CVE-2021-28812	A command injection vulnerability has been reported to affect certain versions of Video Station. If exploited, this vulnerability allows remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Video Station versions prior to 5.5.4 on QTS 4.5.2; versions prior to 5.5.4 on QuTS hero h4.5.2; versions prior to 5.5.4 on QuTScloud c4.5.4. This issue does not affect: QNAP Systems Inc. Video Station on QTS 4.3.6; on QTS 4.3.3.	8.8	More Details
CVE-2020-18264	Cross Site Request Forgery (CSRF) in Simple-Log v1.6 allows remote attackers to gain privilege and execute arbitrary code via the component "Simple-Log/admin/admin.php?act=act_edit_member".	8.8	More Details
CVE-2020-18265	Cross Site Request Forgery (CSRF) in Simple-Log v1.6 allows remote attackers to gain privilege and execute arbitrary code via the component "Simple-Log/admin/admin.php?act=act_add_member".	8.8	More Details
CVE-2021-32673	reg-keygen-git-hash-plugin is a reg-suit plugin to detect the snapshot key to be compare with using Git commit hash. reg-keygen-git-hash-plugin through and including 0.10.15 allow remote attackers to execute of arbitrary commands. Upgrade to version 0.10.16 or later to resolve this issue.	8.8	More Details
CVE-2021-32665	wire-ios is the iOS version of Wire, an open-source secure messaging app. wire-ios versions 3.8.0 and earlier have a bug in which a conversation could be incorrectly set to "unverified. This occurs when: - Self user is added to a new conversation - Self user is added to an existing conversation - All the participants in the conversation were previously marked as verified. The vulnerability is patched in wire-ios version 3.8.1. As a workaround, one can unverify & verify a device in the conversation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27657	Successful exploitation of this vulnerability could give an authenticated Metasys user an unintended level of access to the server file system, allowing them to access or modify system files by sending specifically crafted web messages to the Metasys system. This issue affects: Johnson Controls Metasys version 11.0 and prior versions.	8.8	More Details
CVE-2021-30527	Use after free in WebUI in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30526	Out of bounds write in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.	8.8	More Details
CVE-2021-30525	Use after free in TabGroups in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2015-1877	The open_generic_xdg_mime function in xdg-open in xdg-utils 1.1.0 rc1 in Debian, when using dash, does not properly handle local variables, which allows remote attackers to execute arbitrary commands via a crafted file.	8.8	More Details
CVE-2021-33712	A vulnerability has been identified in Mendix SAML Module (All versions < V2.1.2). The configuration of the SAML module does not properly check various restrictions and validations imposed by an identity provider. This could allow a remote authenticated attacker to escalate privileges.	8.8	More Details
CVE-2021-30524	Use after free in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30521	Heap buffer overflow in Autofill in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2021-30530	Out of bounds memory access in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2021-30535	Double free in ICU in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-31342	The ugeom2d.dll library in all versions of Solid Edge SE2020 before 2020MP14 and all versions of Solid Edge SE2021 before SE2021MP5 lack proper validation of user-supplied data when parsing DFT files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.	8.8	More Details
CVE-2021-30515	Use after free in File API in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30522	Use after free in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30523	Use after free in WebRTC in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.	8.8	More Details
CVE-2021-30520	Use after free in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30519	Use after free in Payments in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious payments app to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30543	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30518	Heap buffer overflow in Reader Mode in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-32674	Zope is an open-source web application server. This advisory extends the previous advisory at https://github.com/zopefoundation/Zope/security/advisories/GHSA-5pr9-v234-jw36 with additional cases of TAL expression traversal vulnerabilities. Most Python modules are not available for using in TAL expressions that you can add through-the-web, for example in Zope Page Templates. This restriction avoids file system access, for example via the 'os' module. But some of the untrusted modules are available indirectly through Python modules that are available for direct use. By default, you need to have the Manager role to add or edit Zope Page Templates through the web. Only sites that allow untrusted users to add/edit Zope Page Templates through the web are at risk. The problem has been fixed in Zope 5.2.1 and 4.6.1. The workaround is the same as for https://github.com/zopefoundation/Zope/security/advisories/GHSA-5pr9-v234-jw36: A site administrator can restrict adding/editing Zope Page Templates through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing Zope Page Templates through the web should be restricted to trusted users only.	8.8	More Details
CVE-2021-30517	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30516	Heap buffer overflow in History in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30514	Use after free in Autofill in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4495	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to bypass security restrictions, caused by improper access control. By sending a specially-crafted request to the REST API, an attacker could exploit this vulnerability to bypass access restrictions, and execute arbitrary actions with administrative privileges. IBM X-Force ID: 182114.	8.8	More Details
CVE-2021-30513	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30512	Use after free in Notifications in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-33815	dwa_uncompress in libavcodec/exr.c in FFmpeg 4.4 allows an out-of-bounds array access because dc_count is not strictly checked.	8.8	More Details
CVE-2021-30510	Use after free in Aura in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30509	Out of bounds write in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page and a crafted Chrome extension.	8.8	More Details
CVE-2021-30508	Heap buffer overflow in Media Feeds in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to enable certain features in Chrome to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-30507	Inappropriate implementation in Offline in Google Chrome on Android prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	8.8	More Details
CVE-2021-30506	Incorrect security UI in Web App Installs in Google Chrome on Android prior to 90.0.4430.212 allowed an attacker who convinced a user to install a web application to inject scripts or HTML into a privileged page via a crafted HTML page.	8.8	More Details
CVE-2021-30542	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-31343	The jutil.dll library in all versions of Solid Edge SE2020 before 2020MP14 and all versions of Solid Edge SE2021 before SE2021MP5 lack proper validation of user-supplied data when parsing DFT files. This could result in an out-of-bounds write past the end of an allocation structure. An attacker could leverage this vulnerability to execute code in the context of the current process.	8.8	More Details
CVE-2021-26474	Various Vembu products allow an attacker to execute a (non-blind) http-only Cross Site Request Forgery (Other products or versions of products in this family may be affected too.)	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31977	Windows Hyper-V Denial of Service Vulnerability	8.6	More Details
CVE-2021-33739	Microsoft DWM Core Library Elevation of Privilege Vulnerability	8.4	More Details
CVE-2021-3546	An out-of-bounds write vulnerability was found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. The flaw occurs while processing the 'VIRTIO_GPU_CMD_GET_CAPSET' command from the guest. It could allow a privileged guest user to crash the QEMU process on the host, resulting in a denial of service condition, or potential code execution with the privileges of the QEMU process.	8.2	More Details
CVE-2021-21558	Dell EMC NetWorker, 18.x, 19.1.x, 19.2.x 19.3.x, 19.4 and 19.4.0.1, contains an Information Disclosure vulnerability. A local administrator of the gstd system may potentially exploit this vulnerability to read LDAP credentials from local logs and use the stolen credentials to make changes to the network domain.	8.2	More Details
CVE-2021-33741	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.2	More Details
CVE-2021-30536	Out of bounds read in V8 in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page.	8.1	More Details
CVE-2021-32641	auth0-lock is Auth0's signin solution. Versions of nauth0-lock before and including `11.30.0` are vulnerable to reflected XSS. An attacker can execute arbitrary code when the library's `flashMessage` feature is utilized and user input or data from URL parameters is incorporated into the `flashMessage` or the library's `languageDictionary` feature is utilized and user input or data from URL parameters is incorporated into the `languageDictionary`. The vulnerability is patched in version 11.30.1.	8.1	More Details
CVE-2020-25716	A flaw was found in Cloudforms. A role-based privileges escalation flaw where export or import of administrator files is possible. An attacker with a specific group can perform actions restricted only to system administrator. This is the affect of an incomplete fix for CVE-2020-10783. The highest threat from this vulnerability is to data confidentiality and integrity. Versions before cfme 5.11.10.1 are affected	8.1	More Details
CVE-2020-36008	OBottle 2.0 in \c\t.php contains an arbitrary file write vulnerability.	8.1	More Details
CVE-2021-1539	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31980	Microsoft Intune Management Extension Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-30511	Out of bounds read in Tab Groups in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page.	8.1	More Details
CVE-2021-33879	Tencent GameLoop before 4.1.21.90 downloaded updates over an insecure HTTP connection. A malicious attacker in an MITM position could spoof the contents of an XML document describing an update package, replacing a download URL with one pointing to an arbitrary Windows executable. Because the only integrity check would be a comparison of the downloaded file's MD5 checksum to the one contained within the XML document, the downloaded executable would then be executed on the victim's machine.	8.1	More Details
CVE-2021-33898	In Invoice Ninja before 4.4.0, there is an unsafe call to unserialize() in app/Ninja/Repositories/AccountRepository.php that may allow an attacker to deserialize arbitrary PHP classes. In certain contexts, this can result in remote code execution. The attacker's input must be hosted at http://www.geoplugin.net (cleartext HTTP), and thus a successful attack requires spoofing that site or obtaining control of it.	8.1	More Details
CVE-2021-1540	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	8.1	More Details
CVE-2020-27302	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices) can lead to remote code execution via the "memcpy" function, when an attacker in Wi-Fi range sends a crafted "Encrypted GTK" value as part of the WPA2 4-way-handshake.	8.0	More Details
CVE-2020-27301	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices) can lead to remote code execution via the "AES_UnWRAP" function, when an attacker in Wi-Fi range sends a crafted "Encrypted GTK" value as part of the WPA2 4-way-handshake.	8.0	More Details
CVE-2018-25015	An issue was discovered in the Linux kernel before 4.14.16. There is a use-after-free in net/sctp/socket.c for a held lock after a peel off, aka CID-a0ff660058b8.	7.8	More Details
CVE-2021-1502	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1503	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. This vulnerability is due to insufficient validation of values in Webex recording files that are in either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details
CVE-2021-3489	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel did not check that the allocated size was smaller than the ringbuf size, allowing an attacker to perform out-of-bounds writes within the kernel and therefore, arbitrary code execution. This issue was fixed via commit 4b81ccebaeee ("bpf, ringbuf: Deny reserve of buffers larger than ringbuf") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced via 457f44363a88 ("bpf: Implement BPF ring buffer and verifier support for it") (v5.8-rc1).	7.8	More Details
CVE-2020-36385	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.	7.8	More Details
CVE-2021-1528	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user.	7.8	More Details
CVE-2021-32460	The Trend Micro Maximum Security 2021 (v17) consumer product is vulnerable to an improper access control vulnerability in the installer which could allow a local attacker to escalate privileges on a target machine. Please note than an attacker must already have local user privileges and access on the machine to exploit this vulnerability.	7.8	More Details
CVE-2019-25045	An issue was discovered in the Linux kernel before 5.0.19. The XFRM subsystem has a use-after-free, related to an xfrm_state_fini panic, aka CID-dbb2483b2a46.	7.8	More Details
CVE-2021-22335	There is a Memory Buffer Improper Operation Limit vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause exceptions in image processing.	7.8	More Details
CVE-2019-14584	Null pointer dereference in Tianocore EDK2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-36387	An issue was discovered in the Linux kernel before 5.8.2. fs/io_uring.c has a use-after-free related to io_async_task_func and ctx reference holding, aka CID-6d816e088c35.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3491	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFERS operation, which led to negative values being usedin mem_rw when reading /proc/<PID>/mem. This could be used to create a heap overflow leading to arbitrary code execution in the kernel. It was addressed via commit d1f82808877b ("io_uring: truncate lengths larger than MAX_RW_COUNT on provide buffers") (v5.13-rc1) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced in ddf0322db79c ("io_uring: add IORING_OP_PROVIDE_BUFFERS") (v5.7-rc1).	7.8	More Details
CVE-2021-3490	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution. This issue was fixed via commit 049c4e13714e ("bpf: Fix alu32 const subreg bound tracking on bitwise operations") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. The AND/OR issues were introduced by commit 3f50f132d840 ("bpf: Verifier, do explicit ALU32 bounds tracking") (5.7-rc1) and the XOR variant was introduced by 2921c90d4718 ("bpf:Fix a verifier failure with xor") (5.10-rc1).	7.8	More Details
CVE-2021-1526	A vulnerability in Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. This vulnerability is due to insufficient validation of values in Webex recording files that are in Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	7.8	More Details
CVE-2021-20259	A flaw was found in the Foreman project. The Proxmox compute resource exposes the password through the API to an authenticated local attacker with view_hosts permission. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. Versions before foreman_fog_proxmox 0.13.1 are affected	7.8	More Details
CVE-2021-24023	An improper input validation in FortiAI v1.4.0 and earlier may allow an authenticated user to gain system shell access via a malicious payload in the "diagnose" command.	7.8	More Details
CVE-2021-31967	VP9 Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31954	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-34280	Polaris Office v9.103.83.44230 is affected by a Uninitialized Pointer Vulnerability in PolarisOffice.exe and EngineDLL.dll that may cause a Remote Code Execution. To exploit the vulnerability, someone must open a crafted PDF file.	7.8	More Details
CVE-2021-31953	Windows Filter Manager Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31952	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27387	A vulnerability has been identified in Simcenter Femap 2020.2 (All versions < V2020.2.MP3), Simcenter Femap 2021.1 (All versions < V2021.1.MP3). The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27399. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12819)	7.8	More Details
CVE-2021-27390	A vulnerability has been identified in JT2Go (All versions < V13.1.0.3), Teamcenter Visualization (All versions < V13.1.0.3). The TIFF_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13131)	7.8	More Details
CVE-2021-31951	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27399	A vulnerability has been identified in Simcenter Femap 2020.2 (All versions < V2020.2.MP3), Simcenter Femap 2021.1 (All versions < V2021.1.MP3). The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27387. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12820)	7.8	More Details
CVE-2021-31946	Paint 3D Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31945	Paint 3D Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31943	3D Viewer Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31942	3D Viewer Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1675	Windows Print Spooler Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31939	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31940	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31956	Windows NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-31941	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31983	Paint 3D Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31985	Microsoft Defender Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-31969	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-31973	Windows GPSVC Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-29091	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in file management component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to write arbitrary files via unspecified vectors.	7.7	More Details
CVE-2021-28807	A post-authentication reflected XSS vulnerability has been reported to affect QNAP NAS running Q'center. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already fixed this vulnerability in the following versions of Q'center: QTS 4.5.3: Q'center v1.12.1012 and later QTS 4.3.6: Q'center v1.10.1004 and later QTS 4.3.3: Q'center v1.10.1004 and later QuTS hero h4.5.2: Q'center v1.12.1012 and later QuTScloud c4.5.4: Q'center v1.12.1012 and later	7.7	More Details
CVE-2021-31964	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-31950	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-31948	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22222	Infinite loop in DVB-S2-BB dissector in Wireshark 3.4.0 to 3.4.5 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2020-29323	The D-link router DIR-885L-MFC 1.15b02, v1.21b05 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	7.5	More Details
CVE-2020-29322	The D-Link router DIR-880L 1.07 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	7.5	More Details
CVE-2020-29324	The DLink Router DIR-895L MFC v1.21b05 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	7.5	More Details
CVE-2020-29321	The D-Link router DIR-868L 3.01 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	7.5	More Details
CVE-2021-28677	An issue was discovered in Pillow before 8.2.0. For EPS data, the readline implementation used in EPSImageFile has to deal with any combination of \r and \n as line endings. It used an accidentally quadratic method of accumulating lines while looking for a line ending. A malicious EPS file could use this to perform a DoS of Pillow in the open phase, before an image was accepted for opening.	7.5	More Details
CVE-2021-29500	bubble fireworks is an open source java package relating to Spring Framework. In bubble fireworks before version 2021.BUILD-SNAPSHOT there is a vulnerability in which the package did not properly verify the signature of JSON Web Tokens. This allows to forgery of valid JWTs.	7.5	More Details
CVE-2021-28676	An issue was discovered in Pillow before 8.2.0. For FLI data, FliDecode did not properly check that the block advance was non-zero, potentially leading to an infinite loop on load.	7.5	More Details
CVE-2021-3530	A flaw was discovered in GNU libiberty within demangle_path() in rust-demangle.c, as distributed in GNU Binutils version 2.36. A crafted symbol can cause stack memory to be exhausted leading to a crash.	7.5	More Details
CVE-2021-31958	Windows NTLM Elevation of Privilege Vulnerability	7.5	More Details
CVE-2021-24340	The WP Statistics WordPress plugin before 13.0.8 relied on using the WordPress esc_sql() function on a field not delimited by quotes and did not first prepare the query. Additionally, the page, which should have been accessible to administrator only, was also available to any visitor, including unauthenticated ones.	7.5	More Details
CVE-2020-14326	A vulnerability was found in RESTEasy, where RootNode incorrectly caches routes. This issue results in hash flooding, leading to slower requests with higher CPU time spent searching and adding the entry. This flaw allows an attacker to cause a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31976	Server for NFS Information Disclosure Vulnerability	7.5	More Details
CVE-2021-31975	Server for NFS Information Disclosure Vulnerability	7.5	More Details
CVE-2021-31974	Server for NFS Denial of Service Vulnerability	7.5	More Details
CVE-2020-14380	An account takeover flaw was found in Red Hat Satellite 6.7.2 onward. A potential attacker with proper authentication to the relevant external authentication source (SSO or Open ID) can claim the privileges of already existing local users of Satellite.	7.5	More Details
CVE-2021-33054	SOGo 2.x before 2.4.1 and 3.x through 5.x before 5.1.1 does not validate the signatures of any SAML assertions it receives. Any actor with network access to the deployment could impersonate users when SAML is the authentication method. (Only versions after 2.0.5a are affected.)	7.5	More Details
CVE-2021-31968	Windows Remote Desktop Services Denial of Service Vulnerability	7.5	More Details
CVE-2021-31701	Mintty before 3.4.7 mishandles Bracketed Paste Mode.	7.5	More Details
CVE-2021-22516	Insertion of Sensitive Information into Log File vulnerability in Micro Focus Secure API Manager (SAPIM) product, affecting version 2.0.0. The vulnerability could lead to sensitive information being in a log file.	7.5	More Details
CVE-2021-28091	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature.	7.5	More Details
CVE-2021-33176	VerneMQ MQTT Broker versions prior to 1.12.0 are vulnerable to a denial of service attack as a result of excessive memory consumption due to the handling of untrusted inputs. These inputs cause the message broker to consume large amounts of memory, resulting in the application being terminated by the operating system.	7.5	More Details
CVE-2021-22313	There is a Security Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	7.5	More Details
CVE-2021-22317	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	7.5	More Details
CVE-2021-22322	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22324	There is a Credentials Management Errors vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	7.5	More Details
CVE-2021-20380	IBM QRadar Advisor With Watson App 1.1 through 2.5 as used on IBM QRadar SIEM 7.4 could allow a remote user to obtain sensitive information from HTTP requests that could aid in further attacks against the system. IBM X-Force ID: 195712.	7.5	More Details
CVE-2021-22336	There is an Improper Control of Generation of Code vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause denial of security services on a rooted device.	7.5	More Details
CVE-2021-28810	If exploited, this vulnerability allows an attacker to access resources which are not otherwise accessible without proper authentication. Roon Labs has already fixed this vulnerability in the following versions: Roon Server 2021-05-18 and later	7.5	More Details
CVE-2021-32926	When an authenticated password change request takes place, this vulnerability could allow the attacker to intercept the message that includes the legitimate, new password hash and replace it with an illegitimate hash. The user would no longer be able to authenticate to the controller (Micro800: All versions, MicroLogix 1400: Version 21 and later) causing a denial-of-service condition	7.5	More Details
CVE-2021-28848	Mintty before 3.4.5 allows remote servers to cause a denial of service (Windows GUI hang) by telling the Mintty window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. In other words, it does not implement a usleep or similar delay upon processing a title change.	7.5	More Details
CVE-2021-33560	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address a side-channel attack against mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPGP.	7.5	More Details
CVE-2020-35970	An issue was discovered in YzmCMS 5.8. There is a SSRF vulnerability in the background collection management that allows arbitrary file read.	7.5	More Details
CVE-2021-28847	MobaXterm before 21.0 allows remote servers to cause a denial of service (Windows GUI hang) via tab title change requests that are sent repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls.	7.5	More Details
CVE-2020-26515	An insufficiently protected credentials issue was discovered in Intland codeBeamer ALM 10.x through 10.1.SP4. The remember-me cookie (CB_LOGIN) issued by the application contains the encrypted user's credentials. However, due to a bug in the application code, those credentials are encrypted using a NULL encryption key.	7.5	More Details
CVE-2021-33175	EMQ X Broker versions prior to 4.2.8 are vulnerable to a denial of service attack as a result of excessive memory consumption due to the handling of untrusted inputs. These inputs cause the message broker to consume large amounts of memory, resulting in the application being terminated by the operating system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22116	RabbitMQ all versions prior to 3.8.16 are prone to a denial of service vulnerability due to improper input validation in AMQP 1.0 client connection endpoint. A malicious user can exploit the vulnerability by sending malicious AMQP messages to the target RabbitMQ instance having the AMQP 1.0 plugin enabled.	7.5	More Details
CVE-2021-22215	An information disclosure vulnerability in GitLab EE versions 13.11 and later allowed a project owner to leak information about the members' on-call rotations in other projects	7.5	More Details
CVE-2021-33571	In Django 2.2 before 2.2.24, 3.x before 3.1.12, and 3.2 before 3.2.4, URLValidator, validate_ipv4_address, and validate_ipv46_address do not prohibit leading zero characters in octal literals. This may allow a bypass of access control that is based on IP addresses. (validate_ipv4_address and validate_ipv46_address are unaffected with Python 3.9.5+..) .	7.5	More Details
CVE-2020-7469	In FreeBSD 12.2-STABLE before r367402, 11.4-STABLE before r368202, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 the handler for a routing option caches a pointer into the packet buffer holding the ICMPv6 message. However, when processing subsequent options the packet buffer may be freed, rendering the cached pointer invalid. The network stack may later dereference the pointer, potentially triggering a use-after-free.	7.5	More Details
CVE-2020-24862	The catID parameter in Pharmacy Medical Store and Sale Point v1.0 has been found to be vulnerable to a Time-Based blind SQL injection via the /medical/inventories.php path which allows attackers to retrieve all databases.	7.5	More Details
CVE-2020-36382	OpenVPN Access Server 2.7.3 to 2.8.7 allows remote attackers to trigger an assert during the user authentication phase via incorrect authentication token data in an early phase of the user authentication resulting in a denial of service.	7.5	More Details
CVE-2020-25362	The id paramater in Online Shopping Alphaware 1.0 has been discovered to be vulnerable to an Error-Based blind SQL injection in the /alphaware/details.php path. This allows an attacker to retrieve all databases.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31340	A vulnerability has been identified in SIMATIC RF166C (All versions > V1.1 and < V1.3.2), SIMATIC RF185C (All versions > V1.1 and < V1.3.2), SIMATIC RF186C (All versions > V1.1 and < V1.3.2), SIMATIC RF186CI (All versions > V1.1 and < V1.3.2), SIMATIC RF188C (All versions > V1.1 and < V1.3.2), SIMATIC RF188CI (All versions > V1.1 and < V1.3.2), SIMATIC RF360R (All versions < V2.0), SIMATIC Reader RF610R CMIIT (All versions > V3.0 < V4.0), SIMATIC Reader RF610R ETSI (All versions > V3.0 < V4.0), SIMATIC Reader RF610R FCC (All versions > V3.0 < V4.0), SIMATIC Reader RF615R CMIIT (All versions > V3.0 < V4.0), SIMATIC Reader RF615R ETSI (All versions > V3.0 < V4.0), SIMATIC Reader RF615R FCC (All versions > V3.0 < V4.0), SIMATIC Reader RF650R ARIB (All versions > V3.0 < V4.0), SIMATIC Reader RF650R CMIIT (All versions > V3.0 < V4.0), SIMATIC Reader RF650R ETSI (All versions > V3.0 < V4.0), SIMATIC Reader RF650R FCC (All versions > V3.0 < V4.0), SIMATIC Reader RF680R ARIB (All versions > V3.0 < V4.0), SIMATIC Reader RF680R CMIIT (All versions > V3.0 < V4.0), SIMATIC Reader RF680R ETSI (All versions > V3.0 < V4.0), SIMATIC Reader RF680R FCC (All versions > V3.0 < V4.0), SIMATIC Reader RF685R ARIB (All versions > V3.0 < V4.0), SIMATIC Reader RF685R CMIIT (All versions > V3.0 < V4.0), SIMATIC Reader RF685R ETSI (All versions > V3.0 < V4.0), SIMATIC Reader RF685R FCC (All versions > V3.0 < V4.0). Affected devices do not properly handle large numbers of incoming connections. An attacker may leverage this to cause a Denial-of-Service situation.	7.5	More Details
CVE-2021-32625	Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. An integer overflow bug in Redis version 6.0 or newer, could be exploited using the STRALGO LCS command to corrupt the heap and potentially result with remote code execution. This is a result of an incomplete fix by CVE-2021-29477. The problem is fixed in version 6.2.4 and 6.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to use ACL configuration to prevent clients from using the STRALGO LCS command. On 64 bit systems which have the fixes of CVE-2021-29477 (6.2.3 or 6.0.13), it is sufficient to make sure that the proto-max-bulk-len config parameter is smaller than 2GB (default is 512MB).	7.5	More Details
CVE-2021-33840	The server in Luca through 1.1.14 allows remote attackers to cause a denial of service (insertion of many fake records related to COVID-19) because Phone Number data lacks a digital signature.	7.5	More Details
CVE-2021-33742	Windows MSHTML Platform Remote Code Execution Vulnerability	7.5	More Details
CVE-2021-33839	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because the QR code of a Public Location can be intentionally confused with the QR code of a Private Meeting.	7.5	More Details
CVE-2021-33838	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because requests related to Check-In State occur shortly after requests for Phone Number Registration.	7.5	More Details
CVE-2020-36009	OBottle 2.0 in \c\g.php contains an arbitrary file download vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22334	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause app redirections.	7.4	More Details
CVE-2021-32923	HashiCorp Vault and Vault Enterprise allowed the renewal of nearly-expired token leases and dynamic secret leases (specifically, those within 1 second of their maximum TTL), which caused them to be incorrectly treated as non-expiring during subsequent use. Fixed in 1.5.9, 1.6.5, and 1.7.2.	7.4	More Details
CVE-2021-31949	Microsoft Outlook Remote Code Execution Vulnerability	7.3	More Details
CVE-2021-31938	Microsoft VsCode Kubernetes Tools Extension Elevation of Privilege Vulnerability	7.3	More Details
CVE-2021-23391	This affects all versions of package calipso. It is possible for a malicious module to overwrite files on an arbitrary file system through the module install functionality.	7.3	More Details
CVE-2021-3277	Nagios XI 5.7.5 and earlier allows authenticated admins to upload arbitrary files due to improper validation of the rename functionality in custom-includes component, which leads to remote code execution by uploading php files.	7.2	More Details
CVE-2021-31966	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2021-24336	The FlightLog WordPress plugin through 3.0.2 does not sanitise, validate or escape various POST parameters before using them a SQL statement, leading to SQL injections exploitable by editor and administrator users	7.2	More Details
CVE-2021-32670	Datasette is an open source multi-tool for exploring and publishing data. The `?_trace=1` debugging feature in Datasette does not correctly escape generated HTML, resulting in a [reflected cross-site scripting](https://owasp.org/www-community/attacks/xss/#reflected-xss-attacks) vulnerability. This vulnerability is particularly relevant if your Datasette installation includes authenticated features using plugins such as [datasette-auth-passwords](https://datasette.io/plugins/datasette-auth-passwords) as an attacker could use the vulnerability to access protected data. Datasette 0.57 and 0.56.1 both include patches for this issue. If you run Datasette behind a proxy you can workaround this issue by rejecting any incoming requests with `?_trace=` or `&_trace=` in their query string parameters.	7.2	More Details
CVE-2021-28811	If exploited, this command injection vulnerability could allow remote attackers to run arbitrary commands. Roon Labs has already fixed this vulnerability in the following versions: Roon Server 2021-05-18 and later	7.2	More Details
CVE-2021-29090	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in PHP component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to execute arbitrary SQL command via unspecified vectors.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3529	A flaw was found in noobaa-core in versions before 5.7.0. This flaw results in the name of an arbitrarily URL being copied into an HTML document as plain text between tags, including potentially a payload script. The input was echoed unmodified in the application response, resulting in arbitrary JavaScript being injected into an application's response. The highest threat to the system is for confidentiality, availability, and integrity.	7.1	More Details
CVE-2018-10195	lrzsz before version 0.12.21~rc can leak information to the receiving side due to an incorrect length check in the function zsdata that causes a size_t to wrap around.	7.1	More Details
CVE-2021-21559	Dell EMC NetWorker, versions 18.x, 19.1.x, 19.2.x 19.3.x, 19.4, and 19.4.0.1 contain an Improper Certificate Validation vulnerability in the client (NetWorker Management Console) components which uses SSL encrypted connection in order to communicate with the application server. An unauthenticated attacker in the same network collision domain as the NetWorker Management Console client could potentially exploit this vulnerability to perform man-in-the-middle attacks to intercept and tamper the traffic between the client and the application server.	7.1	More Details
CVE-2020-36386	An issue was discovered in the Linux kernel before 5.8.1. net/bluetooth/hci_event.c has a slab out-of-bounds read in hci_extended_inquiry_result_evt, aka CID-51c19bf3d5cf.	7.1	More Details
CVE-2021-31963	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.1	More Details
CVE-2020-10771	A flaw was found in Infinispan version 10, where it is possible to perform various actions that could have side effects using GET requests. This flaw allows an attacker to perform a cross-site request forgery (CSRF) attack.	7.1	More Details
CVE-2021-26420	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.1	More Details
CVE-2020-35514	An insecure modification flaw in the /etc/kubernetes/kubeconfig file was found in OpenShift. This flaw allows an attacker with access to a running container which mounts /etc/kubernetes or has local access to the node, to copy this kubeconfig file and attempt to add their own node to the OpenShift cluster. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. This flaw affects versions before openshift4/ose-machine-config-operator v4.7.0-202105111858.p0.	7.0	More Details
CVE-2020-1742	An insecure modification vulnerability flaw was found in containers using nmstate/kubernetes-nmstate-handler. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. Versions before kubernetes-nmstate-handler-container-v2.3.0-30 are affected.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32661	Backstage is an open platform for building developer portals. In versions of Backstage's Techdocs Plugin (`@backstage/plugin-techdocs`) prior to 0.9.5, a malicious internal actor can potentially upload documentation content with malicious scripts by embedding the script within an `object` element. This may give access to sensitive data when other users visit that same documentation page. The ability to upload malicious content may be limited by internal code review processes, unless the chosen TechDocs deployment method is to use an object store and the actor has access to upload files directly to that store. The vulnerability is patched in the `0.9.5` release of `@backstage/plugin-techdocs`.	6.8	More Details
CVE-2021-31971	Windows HTML Platforms Security Feature Bypass Vulnerability	6.8	More Details
CVE-2021-32660	Backstage is an open platform for building developer portals, and techdocs-common contains common functionalities for Backstage's TechDocs. In versions of `@backstage/tehdocs-common` prior to 0.6.4, a malicious internal actor is able to upload documentation content with malicious scripts. These scripts would normally be sanitized by the TechDocs frontend, but by tricking a user to visit the content via the TechDocs API, the content sanitazion will be bypassed. If the TechDocs API is hosted on the same origin as the Backstage app or other backend plugins, this may give access to sensitive data. The ability to upload malicious content may be limited by internal code review processes, unless the chosen TechDocs deployment method is to use an object store and the actor has access to upload files directly to that store. The vulnerability is patched in the `0.6.4` release of `@backstage/techdocs-common`.	6.8	More Details
CVE-2021-22316	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Attackers with physical access to the device can thereby exploit this vulnerability. A successful exploitation of this vulnerability can compromise the device's data security and functional availability.	6.8	More Details
CVE-2021-26928	BIRD through 2.0.7 does not provide functionality for password authentication of BGP peers. Because of this, products that use BIRD (which may, for example, include Tigera products in some configurations, as well as products of other vendors) may have been susceptible to route redirection for Denial of Service and/or Information Disclosure. NOTE: a researcher has asserted that the behavior is within Tigera’s area of responsibility; however, Tigera disagrees	6.8	More Details
CVE-2021-22214	When requests to the internal network for webhooks are enabled, a server-side request forgery vulnerability in GitLab CE/EE affecting all versions starting from 10.5 was possible to exploit for an unauthenticated attacker even on a GitLab instance where registration is limited	6.8	More Details
CVE-2021-22130	A stack-based buffer overflow vulnerability in FortiProxy physical appliance CLI 2.0.0 to 2.0.1, 1.2.0 to 1.2.9, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 may allow an authenticated, remote attacker to perform a Denial of Service attack by running the `diagnose sys cpuset` with a large cpuset mask value. Fortinet is not aware of any successful exploitation of this vulnerability that would lead to code execution.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22221	An issue has been discovered in GitLab affecting all versions starting from 12.9.0 before 13.10.5, all versions starting from 13.11.0 before 13.11.5, all versions starting from 13.12.0 before 13.12.2. Insufficient expired password validation in various operations allow user to maintain limited access after their password expired	6.5	More Details
CVE-2021-22217	A denial of service vulnerability in all versions of GitLab CE/EE before 13.12.2, 13.11.5 or 13.10.5 allows an attacker to cause uncontrolled resource consumption with a specially crafted issue or merge request	6.5	More Details
CVE-2020-28713	Incorrect access control in push notification service in Night Owl Smart Doorbell FW version 20190505 allows remote users to send push notification events via an exposed PNS server. A remote attacker can passively record push notification events which are sent over an insecure web request. The web service does not authenticate requests, and allows attackers to send an indefinite amount of motion or doorbell events to a user's mobile application by either replaying or deliberately crafting false events.	6.5	More Details
CVE-2020-21005	WellCMS 2.0 beta3 is vulnerable to File Upload. A user can log in to the CMS background and upload a picture. Because the upload file type is controllable, the user can modify the upload file type to get webshell.	6.5	More Details
CVE-2021-20371	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516.	6.5	More Details
CVE-2021-22549	An attacker can modify the address to point to trusted memory to overwrite arbitrary trusted memory. It is recommended to update past 0.6.2 or git commit https://github.com/google/asylo/commit/53ed5d8fd8118ced1466e509606dd2f473707a5c	6.5	More Details
CVE-2021-22548	An attacker can change the pointer to untrusted memory to point to trusted memory region which causes copying trusted memory to trusted memory, if the latter is later copied out, it allows for reading of memory regions from the trusted region. It is recommended to update past 0.6.2 or git commit https://github.com/google/asylo/commit/53ed5d8fd8118ced1466e509606dd2f473707a5c	6.5	More Details
CVE-2021-22216	A denial of service vulnerability in all versions of GitLab CE/EE before 13.12.2, 13.11.5 or 13.10.5 allows an attacker to cause uncontrolled resource consumption with a very long issue or merge request description	6.5	More Details
CVE-2020-1750	A flaw was found in the machine-config-operator that causes an OpenShift node to become unresponsive when a container consumes a large amount of memory. An attacker could use this flaw to deny access to schedule new pods in the OpenShift cluster. This was fixed in openshift/machine-config-operator 4.4.3, openshift/machine-config-operator 4.3.25, openshift/machine-config-operator 4.2.36.	6.5	More Details
CVE-2021-30540	Incorrect security UI in payments in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	6.5	More Details
CVE-2020-26136	In SilverStripe through 4.6.0-rc1, GraphQL doesn't honour MFA (multi-factor authentication) when using basic authentication.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31249	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components.	6.5	More Details
CVE-2020-4732	IBM Jazz Foundation and IBM Engineering products could allow an authenticated user to obtain sensitive information due to lack of security restrictions. IBM X-Force ID: 188126.	6.5	More Details
CVE-2020-22048	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the ff_frame_pool_get function in framepool.c.	6.5	More Details
CVE-2020-14336	A flaw was found in the Restricted Security Context Constraints (SCC), where it allows pods to craft custom network packets. This flaw allows an attacker to cause a denial of service attack on an OpenShift Container Platform cluster if they can deploy pods. The highest threat from this vulnerability is to system availability.	6.5	More Details
CVE-2020-14371	A credential leak vulnerability was found in Red Hat Satellite. This flaw exposes the compute resources credentials through VMs that are running on these resources in Satellite.	6.5	More Details
CVE-2021-24012	An improper following of a certificate's chain of trust vulnerability in FortiGate versions 6.4.0 to 6.4.4 may allow an LDAP user to connect to SSLVPN with any certificate that is signed by a trusted Certificate Authority.	6.5	More Details
CVE-2021-3544	Several memory leaks were found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. They exist in contrib/vhost-user-gpu/vhost-user-gpu.c and contrib/vhost-user-gpu/virgl.c due to improper release of memory (i.e., free) after effective lifetime.	6.5	More Details
CVE-2021-3545	An information disclosure vulnerability was found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. The flaw exists in virgl_cmd_get_capset_info() in contrib/vhost-user-gpu/virgl.c and could occur due to the read of uninitialized memory. A malicious guest could exploit this issue to leak memory from the host.	6.5	More Details
CVE-2019-12067	The ahci_commit_buf function in ide/ahci.c in QEMU allows attackers to cause a denial of service (NULL dereference) when the command header 'ad->cur_cmd' is null.	6.5	More Details
CVE-2020-22046	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the avpriv_float_dsp_allocl function in libavutil/float_dsp.c.	6.5	More Details
CVE-2020-22049	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the wtvfile_open_sector function in wtvdec.c.	6.5	More Details
CVE-2020-22056	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the config_input function in af_acrossover.c.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27661	A divide-by-zero issue was found in dwc2_handle_packet in hw/usb/hcd-dwc2.c in the hcd-dwc2 USB host controller emulation of QEMU. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service.	6.5	More Details
CVE-2020-6950	Directory traversal in Eclipse Mojarra before 2.3.14 allows attackers to read arbitrary files via the loc parameter or con parameter.	6.5	More Details
CVE-2021-31855	KDE Messagelib through 5.17.0 reveals cleartext of encrypted messages in some situations. Deleting an attachment of a decrypted encrypted message stored on a remote server (e.g., an IMAP server) causes KMail to upload the decrypted content of the message to the remote server. With a crafted message, a user could be tricked into decrypting an encrypted message and then deleting an attachment attached to this message. If the attacker has access to the messages stored on the email server, then the attacker could read the decrypted content of the encrypted message. This occurs in ViewerPrivate::deleteAttachment in messageviewer/src/viewer/viewer_p.cpp.	6.5	More Details
CVE-2020-22051	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the filter_frame function in vf_tile.c.	6.5	More Details
CVE-2021-31807	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. An integer overflow problem allows a remote server to achieve Denial of Service when delivering responses to HTTP Range requests. The issue trigger is a header that can be expected to exist in HTTP traffic without any malicious intent.	6.5	More Details
CVE-2021-30533	Insufficient policy enforcement in PopupBlocker in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted iframe.	6.5	More Details
CVE-2020-22054	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the av_dict_set function in dict.c.	6.5	More Details
CVE-2021-30534	Insufficient policy enforcement in iFrameSandbox in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2021-22550	An attacker can modify the pointers in enclave memory to overwrite arbitrary memory addresses within the secure enclave. It is recommended to update past 0.6.3 or git commit https://github.com/google/asylo/commit/a47ef55db2337d29de19c50cd29b0deb2871d31c	6.5	More Details
CVE-2021-32666	wire-ios is the iOS version of Wire, an open-source secure messaging app. In wire-ios versions 3.8.0 and prior, a vulnerability exists that can cause a denial of service between users. If a user has an invalid assetID for their profile picture and it contains the " character, it will cause the iOS client to crash. The vulnerability is patched in wire-ios version 3.8.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1690	An improper authorization flaw was discovered in openstack-selinux's applied policy where it does not prevent a non-root user in a container from privilege escalation. A non-root attacker in one or more Red Hat OpenStack (RHOSP) containers could send messages to the dbus. With access to the dbus, the attacker could start or stop services, possibly causing a denial of service. Versions before openstack-selinux 0.8.24 are affected.	6.5	More Details
CVE-2021-1563	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2020-36006	AppCMS 2.0.101 in /admin/info.php has an arbitrary file deletion vulnerability which allows attackers to delete arbitrary files on the site.	6.5	More Details
CVE-2020-36004	AppCMS 2.0.101 in /admin/download_frame.php has a SQL injection vulnerability which allows attackers to obtain sensitive database information.	6.5	More Details
CVE-2021-26994	Clustered Data ONTAP versions prior to 9.7P13 and 9.8P3 are susceptible to a vulnerability which could allow single workloads to cause a Denial of Service (DoS) on a cluster node.	6.5	More Details
CVE-2021-32662	Backstage is an open platform for building developer portals, and techdocs-common contains common functionalities for Backstage's TechDocs. In `@backstage/techdocs-common` versions prior to 0.6.3, a malicious actor could read sensitive files from the environment where TechDocs documentation is built and published by setting a particular path for `docs_dir` in `mkdocs.yml`. These files would then be available over the TechDocs backend API. This vulnerability is mitigated by the fact that an attacker would need access to modify the `mkdocs.yml` in the documentation source code, and would also need access to the TechDocs backend API. The vulnerability is patched in the `0.6.3` release of `@backstage/techdocs-common`.	6.5	More Details
CVE-2020-36005	AppCMS 2.0.101 in /admin/app.php has an arbitrary file deletion vulnerability which allows attackers to delete arbitrary files on the site.	6.5	More Details
CVE-2020-36142	BloofoxCMS 0.5.2.1 allows Directory traversal vulnerability by inserting '../' payloads within the 'fileurl' parameter.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1564	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	6.5	More Details
CVE-2020-36140	BloofoxCMS 0.5.2.1 allows Cross-Site Request Forgery (CSRF) via 'mode=settings&page=editor', as demonstrated by use of 'mode=settings&page=editor' to change any file content (Locally/Remotely).	6.5	More Details
CVE-2021-30531	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	6.5	More Details
CVE-2021-31959	Scripting Engine Memory Corruption Vulnerability	6.4	More Details
CVE-2020-14388	A flaw was found in the Red Hat 3scale API Management Platform, where member permissions for an API's admin portal were not properly enforced. This flaw allows an authenticated user to bypass normal account restrictions and access API services where they do not have permission.	6.3	More Details
CVE-2021-1537	A vulnerability in the installer software of Cisco ThousandEyes Recorder could allow an unauthenticated, local attacker to access sensitive information that is contained in the ThousandEyes Recorder installer software. This vulnerability exists because sensitive information is included in the application installer. An attacker could exploit this vulnerability by downloading the installer and extracting its contents. A successful exploit could allow the attacker to access sensitive information that is included in the application installer.	6.2	More Details
CVE-2011-3656	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.6.24 and 4.x through 7 allows remote attackers to inject arbitrary web script or HTML via vectors involving HTTP 0.9 errors, non-default ports, and content-sniffing.	6.1	More Details
CVE-2021-33904	In Accela Civic Platform through 21.1, the security/hostSignon.do parameter servProvCode is vulnerable to XSS. NOTE: The vendor states "there are configurable security flags and we are unable to reproduce them with the available information.	6.1	More Details
CVE-2021-26584	A security vulnerability in HPE OneView for VMware vCenter (OV4VC) could be exploited remotely to allow Cross-Site Scripting. HPE has released the following software update to resolve the vulnerability in HPE OneView for VMware vCenter (OV4VC).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24342	The JNews WordPress theme before 8.0.6 did not sanitise the cat_id parameter in the POST request /?ajax-request=jnews (with action=jnews_build_mega_category_*), leading to a Reflected Cross-Site Scripting (XSS) issue.	6.1	More Details
CVE-2021-31252	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it.	6.1	More Details
CVE-2020-36007	AppCMS 2.0.101 in /admin/template/tpl_app.php has a cross site scripting attack vulnerability which allows the attacker to obtain sensitive information of other users.	6.1	More Details
CVE-2020-36384	PageLayer before 1.3.5 allows reflected XSS via color settings.	6.1	More Details
CVE-2020-18268	Open Redirect in Z-BlogPHP v1.5.2 and earlier allows remote attackers to obtain sensitive information via the "redirect" parameter in the component "zb_system/cmd.php."	6.1	More Details
CVE-2020-26885	An issue was discovered in 2sic 2sxc before 11.22. A XSS vulnerability in the sxcver parameter of dnn/ui.html allows an attacker to craft a malicious URL that executes a JavaScript payload in a victim's browser.	6.1	More Details
CVE-2021-22220	An issue has been discovered in GitLab affecting all versions starting with 13.10. GitLab was vulnerable to a stored XSS in blob viewer of notebooks.	6.1	More Details
CVE-2021-26080	EditworkflowScheme.jspa in Jira Server and Jira Data Center before version 8.5.14, and from version 8.6.0 before version 8.13.6, and from 8.14.0 before 8.16.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-31738	Adiscon LogAnalyzer 4.1.10 and 4.1.11 allow login.php XSS.	6.1	More Details
CVE-2021-26078	The number range searcher component in Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before version 8.13.6, and from version 8.14.0 before version 8.16.1 allows remote attackers inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-26079	The CardLayoutConfigTable component in Jira Server and Jira Data Center before version 8.5.15, and from version 8.6.0 before version 8.13.7, and from version 8.14.0 before 8.17.0 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-36383	PageLayer before 1.3.5 allows reflected XSS via the font-size parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32015	In Nuvoton NPCT75x TPM 1.2 firmware 7.4.0.0, a local authenticated malicious user with high privileges could potentially gain unauthorized access to TPM non-volatile memory. NOTE: Upgrading to firmware version 7.4.0.1 will mitigate against the vulnerability, but version 7.4.0.1 is not TCG or Common Criteria (CC) certified. Nuvoton recommends that users apply the NPCT75x TPM 1.2 firmware update.	6.0	More Details
CVE-2020-10742	A flaw was found in the Linux kernel. An index buffer overflow during Direct IO write leading to the NFS client to crash. In some cases, a reach out of the index after one memory allocation by kmalloc will cause a kernel panic. The highest threat from this vulnerability is to data confidentiality and system availability.	6.0	More Details
CVE-2020-35503	A NULL pointer dereference flaw was found in the megasas-gen2 SCSI host bus adapter emulation of QEMU in versions before and including 6.0. This issue occurs in the megasas_command_cancelled() callback function while dropping a SCSI request. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	6.0	More Details
CVE-2021-3565	A flaw was found in tpm2-tools in versions before 5.1.1 and before 4.3.2. tpm2_import used a fixed AES key for the inner wrapper, potentially allowing a MITM attacker to unwrap the inner portion and reveal the key being imported. The highest threat from this vulnerability is to data confidentiality.	5.9	More Details
CVE-2021-33880	The aaugustin websockets library before 9.1 for Python has an Observable Timing Discrepancy on servers when HTTP Basic Authentication is enabled with basic_auth_protocol_factory(credentials=...). An attacker may be able to guess a password via a timing attack.	5.9	More Details
CVE-2021-31957	ASP.NET Core Denial of Service Vulnerability	5.9	More Details
CVE-2020-35510	A flaw was found in jboss-remoting in versions before 5.0.20.SP1-redhat-00001. A malicious attacker could cause threads to hold up forever in the EJB server by writing a sequence of bytes corresponding to the expected messages of a successful EJB client request, but omitting the ACK messages, or just tamper with jboss-remoting code, deleting the lines that send the ACK message from the EJB client code resulting in a denial of service. The highest threat from this vulnerability is to system availability.	5.9	More Details
CVE-2020-14340	A vulnerability was discovered in XNIO where file descriptor leak caused by growing amounts of NIO Selector file handles between garbage collection cycles. It may allow the attacker to cause a denial of service. It affects XNIO versions 3.6.0.Beta1 through 3.8.1.Final.	5.9	More Details
CVE-2021-31830	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to embed JavaScript code when configuring the name of a database to be monitored. This would be triggered when any authorized user logs into the DBSec interface and opens the properties configuration page for this database.	5.9	More Details
CVE-2021-31965	Microsoft SharePoint Server Information Disclosure Vulnerability	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28806	A DOM-based XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.3.1652 Build 20210428. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 Build 20210414. QNAP Systems Inc. QuTScloud versions prior to c4.5.5.1656 Build 20210503. This issue does not affect: QNAP Systems Inc. QTS 4.3.6; 4.3.3.	5.7	More Details
CVE-2021-3499	A vulnerability was found in OVN Kubernetes in versions up to and including 0.3.0 where the Egress Firewall does not reliably apply firewall rules when there is multiple DNS rules. It could lead to potentially lose of confidentiality, integrity or availability of a service.	5.6	More Details
CVE-2021-31972	Event Tracing for Windows Information Disclosure Vulnerability	5.5	More Details
CVE-2021-1544	A vulnerability in logging mechanisms of Cisco Webex Meetings client software could allow an authenticated, local attacker to gain access to sensitive information. This vulnerability is due to unsafe logging of application actions. An attacker could exploit this vulnerability by logging onto the local system and accessing files containing the logged details. A successful exploit could allow the attacker to gain access to sensitive information, including meeting data and recorded meeting transcriptions.	5.5	More Details
CVE-2021-3468	A flaw was found in avahi in versions 0.6 up to 0.8. The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. The highest threat from this vulnerability is to the availability of the avahi service, which becomes unresponsive after this flaw is triggered.	5.5	More Details
CVE-2021-31960	Windows Bind Filter Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2020-14317	It was found that the issue for security flaw CVE-2019-3805 appeared again in a further version of JBoss Enterprise Application Platform - Continuous Delivery (EAP-CD) introducing regression. An attacker could exploit this by modifying the PID file in /var/run/jboss-eap/ allowing the init.d script to terminate any process as root.	5.5	More Details
CVE-2021-31978	Microsoft Defender Denial of Service Vulnerability	5.5	More Details
CVE-2021-23215	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR.	5.5	More Details
CVE-2021-28678	An issue was discovered in Pillow before 8.2.0. For BLP data, BlpImagePlugin did not properly check that reads (after jumping to file offsets) returned data. This could lead to a DoS where the decoder could be run a large number of times on empty data.	5.5	More Details
CVE-2021-3522	GStreamer before 1.18.4 may perform an out-of-bounds read when handling certain ID3v2 tags.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28675	An issue was discovered in Pillow before 8.2.0. PSDImagePlugin.PsdImageFile lacked a sanity check on the number of input layers relative to the size of the data block. This could lead to a DoS on Image.open prior to Image.load.	5.5	More Details
CVE-2021-3569	A stack corruption bug was found in libtpms in versions before 0.7.2 and before 0.8.0 while decrypting data using RSA. This flaw could result in a SIGBUS (bad memory access) and termination of swtpm. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2021-31955	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2021-31970	Windows TCP/IP Driver Security Feature Bypass Vulnerability	5.5	More Details
CVE-2021-3564	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.	5.5	More Details
CVE-2021-26945	An integer overflow leading to a heap-buffer overflow was found in OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR.	5.5	More Details
CVE-2021-26260	An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. This is a different flaw from CVE-2021-23215.	5.5	More Details
CVE-2020-14335	A flaw was found in Red Hat Satellite, which allows a privileged attacker to read OMAPI secrets through the ISC DHCP of Smart-Proxy. This flaw allows an attacker to gain control of DHCP records from the network. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2020-1719	A flaw was found in wildfly. The EJBContext principle is not popped back after invoking another EJB using a different Security Domain. The highest threat from this vulnerability is to data confidentiality and integrity. Versions before wildfly 20.0.0.Final are affected.	5.4	More Details
CVE-2021-28382	Zoho ManageEngine Key Manager Plus before 6001 allows Stored XSS on the user-management page while importing malicious user details from AD.	5.4	More Details
CVE-2020-4977	IBM Engineering Lifecycle Optimization - Publishing is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 192470.	5.4	More Details
CVE-2020-5030	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 193737.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31250	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi.	5.4	More Details
CVE-2021-20346	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595.	5.4	More Details
CVE-2020-35971	A storage XSS vulnerability is found in YzmCMS v5.8, which can be used by attackers to inject JS code and attack malicious XSS on the /admin/system_manage/user_config_edit.html page.	5.4	More Details
CVE-2021-29670	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199408.	5.4	More Details
CVE-2021-29668	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199406.	5.4	More Details
CVE-2021-20348	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597.	5.4	More Details
CVE-2021-32106	In ICEcoder 8.0 allows, a reflected XSS vulnerability was identified in the multipe-results.php page due to insufficient sanitization of the _GET['replace'] variable. As a result, arbitrary Javascript code can get executed.	5.4	More Details
CVE-2021-20347	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596.	5.4	More Details
CVE-2020-35973	An issue was discovered in zzcms2020. There is a XSS vulnerability that can insert and execute JS code arbitrarily via /user/manage.php.	5.4	More Details
CVE-2021-30539	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	5.4	More Details
CVE-2021-20345	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20343	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593.	5.4	More Details
CVE-2020-36139	BloofoxCMS 0.5.2.1 allows Reflected Cross-Site Scripting (XSS) vulnerability by inserting a XSS payload within the 'fileurl' parameter.	5.4	More Details
CVE-2021-3469	Foreman versions before 2.3.4 and before 2.4.0 is affected by an improper authorization handling flaw. An authenticated attacker can impersonate the foreman-proxy if product enable the Puppet Certificate authority (CA) to sign certificate requests that have subject alternative names (SANs). Foreman do not enable SANs by default and `allow-authorization-extensions` is set to `false` unless user change `/etc/puppetlabs/puppetserver/conf.d/ca.conf` configuration explicitly.	5.4	More Details
CVE-2021-20338	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194449.	5.4	More Details
CVE-2021-22337	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause leaking of user click data.	5.3	More Details
CVE-2021-33190	In Apache APISIX Dashboard version 2.6, we changed the default value of listen host to 0.0.0.0 in order to facilitate users to configure external network access. In the IP allowed list restriction, a risky function was used for the IP acquisition, which made it possible to bypass the network limit. At the same time, the default account and password are fixed.Ultimately these factors lead to the issue of security risks. This issue is fixed in APISIX Dashboard 2.6.1	5.3	More Details
CVE-2021-22325	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may result in video streams being intercepted during transmission.	5.3	More Details
CVE-2020-28469	This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosure containing path separator.	5.3	More Details
CVE-2021-23392	The package locutus before 2.0.15 are vulnerable to Regular Expression Denial of Service (ReDoS) via the gopher_parsedir function.	5.3	More Details
CVE-2021-30357	SSL Network Extender Client for Linux before build 800008302 reveals part of the contents of the configuration file supplied, which allows partially disclosing files to which the user did not have access.	5.3	More Details
CVE-2020-15077	OpenVPN Access Server 2.8.7 and earlier versions allows a remote attackers to bypass authentication and access control channel data on servers configured with deferred authentication, which can be used to potentially trigger further information leaks.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29621	Flask-AppBuilder is a development framework, built on top of Flask. User enumeration in database authentication in Flask-AppBuilder <= 3.2.3. Allows for a non authenticated user to enumerate existing accounts by timing the response time from the server when you are logging in. Upgrade to version 3.3.0 or higher to resolve.	5.3	More Details
CVE-2021-33896	Dino before 0.1.2 and 0.2.x before 0.2.1 allows Directory Traversal (only for creation of new files) via URI-encoded path separators.	5.3	More Details
CVE-2021-1527	A vulnerability in Cisco Webex Player for Windows and MacOS could allow an attacker to cause the affected software to terminate or to gain access to memory state information that is related to the vulnerable application. The vulnerability is due to insufficient validation of values in Webex recording files that are stored in Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a malicious WRF file to a user as a link or email attachment and then persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to crash the affected software and view memory state information.	5.3	More Details
CVE-2021-29099	A SQL injection vulnerability exists in some configurations of ArcGIS Server versions 10.8.1 and earlier. Specially crafted web requests can expose information that is not intended to be disclosed (not customer datasets). Web Services that use file based data sources (file Geodatabase or Shape Files or tile cached services) are unaffected by this issue.	5.3	More Details
CVE-2020-5008	IBM DataPower Gateway 10.0.0.0 through 10.0.1.0 and 2018.4.1.0 through 2018.4.1.14 stores sensitive information in GET request parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 193033.	5.3	More Details
CVE-2020-26138	In SilverStripe through 4.6.0-rc1, a FormField with square brackets in the field name skips validation.	5.3	More Details
CVE-2021-31201	Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability	5.2	More Details
CVE-2021-31199	Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability	5.2	More Details
CVE-2021-31944	3D Viewer Information Disclosure Vulnerability	5.0	More Details
CVE-2021-1517	A vulnerability in the multimedia viewer feature of Cisco Webex Meetings and Cisco Webex Meetings Server could allow an authenticated, remote attacker to bypass security protections. This vulnerability is due to unsafe handling of shared content within the multimedia viewer feature. An attacker could exploit this vulnerability by sharing a file through the multimedia viewer feature. A successful exploit could allow the attacker to bypass security protections and prevent warning dialogs from appearing before files are offered to other users.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31831	Incorrect access to deleted scripts vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to gain access to signed SQL scripts which have been marked as deleted or expired within the administrative console. This access was only available through the REST API.	4.9	More Details
CVE-2021-33203	Django before 2.2.24, 3.x before 3.1.12, and 3.2.x before 3.2.4 has a potential directory traversal via django.contrib.admindocs. Staff members could use the TemplateDetailView view to check the existence of arbitrary files. Additionally, if (and only if) the default admindocs templates have been customized by application developers to also show file contents, then not only the existence but also the file contents would have been exposed. In other words, there is directory traversal outside of the template root directories.	4.9	More Details
CVE-2021-26414	Windows DCOM Server Security Feature Bypass	4.8	More Details
CVE-2021-24343	The iFlyChat WordPress plugin before 4.7.0 does not sanitise its APP ID setting before outputting it back in the page, leading to an authenticated Stored Cross-Site Scripting issue	4.8	More Details
CVE-2021-1536	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account.	4.8	More Details
CVE-2020-26517	A cross-site scripting (XSS) issue was discovered in Intland codeBeamer ALM 10.x through 10.1.SP4. It is possible to perform XSS attacks through using the WebDAV functionality to upload files to a project (Authn users), using the users import functionality (Admin only), and changing the login text in the application configuration (Admin only).	4.8	More Details
CVE-2020-25817	SilverStripe through 4.6.0-rc1 has an XXE Vulnerability in CSSContentParser. A developer utility meant for parsing HTML within unit tests can be vulnerable to XML External Entity (XXE) attacks. When this developer utility is misused for purposes involving external or user submitted data in custom project code, it can lead to vulnerabilities such as XSS on HTML output rendered through this custom code. This is now mitigated by disabling external entities during parsing. (The correct CVE ID year is 2020 [CVE-2020-25817, not CVE-2021-25817]).	4.8	More Details
CVE-2021-24344	The Easy Preloader WordPress plugin through 1.0.0 does not sanitise its setting fields, leading to authenticated (admin+) Stored Cross-Site scripting issues	4.8	More Details
CVE-2020-21003	Pbootcms v2.0.3 is vulnerable to Cross Site Scripting (XSS) via admin.php.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32658	Nextcloud Android is the Android client for the Nextcloud open source home cloud system. Due to a timeout issue the Android client may not properly clean all sensitive data on account removal. This could include sensitive key material such as the End-to-End encryption keys. It is recommended that the Nextcloud Android App is upgraded to 3.16.1	4.7	More Details
CVE-2021-1538	A vulnerability in the configuration dashboard of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to execute arbitrary code. This vulnerability is due to insufficient sanitization of configuration entries. An attacker could exploit this vulnerability by logging in as a super admin and entering crafted input to configuration options on the CSPC configuration dashboard. A successful exploit could allow the attacker to execute remote code as root.	4.7	More Details
CVE-2021-1525	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to redirect users to a malicious file. This vulnerability is due to improper validation of URL paths in the application interface. An attacker could exploit this vulnerability by persuading a user to follow a specially crafted URL that is designed to cause Cisco Webex Meetings to include a remote file in the web UI. A successful exploit could allow the attacker to cause the application to offer a remote file to a user, which could allow the attacker to conduct further phishing or spoofing attacks.	4.7	More Details
CVE-2021-22219	All versions of GitLab CE/EE starting from 9.5 before 13.10.5, all versions starting from 13.11 before 13.11.5, and all versions starting from 13.12 before 13.12.2 allow a high privilege user to obtain sensitive information from log files because the sensitive information was not correctly registered for log masking.	4.4	More Details
CVE-2021-30532	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	4.3	More Details
CVE-2020-35972	An issue was discovered in YzmCMS V5.8. There is a CSRF vulnerability that can add member user accounts via member/member/add.html.	4.3	More Details
CVE-2021-30537	Insufficient policy enforcement in cookies in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass cookie policy via a crafted HTML page.	4.3	More Details
CVE-2020-10743	It was discovered that OpenShift Container Platform's (OCP) distribution of Kibana could open in an iframe, which made it possible to intercept and manipulate requests. This flaw allows an attacker to trick a user into performing arbitrary actions in OCP's distribution of Kibana, such as clickjacking.	4.3	More Details
CVE-2017-8761	In OpenStack Swift through 2.10.1, 2.11.0 through 2.13.0, and 2.14.0, the proxy-server logs full tempurl paths, potentially leaking reusable tempurl signatures to anyone with read access to these logs. All Swift deployments using the tempurl middleware are affected.	4.3	More Details
CVE-2020-6641	Two authorization bypass through user-controlled key vulnerabilities in the Fortinet FortiPresence 2.1.0 administration interface may allow an attacker to gain access to some user data via portal manager or portal users parameters.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30538	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.	4.3	More Details
CVE-2021-33881	On NXP MIFARE Ultralight and NTAG cards, an attacker can interrupt a write operation (aka conduct a "tear off" attack) over RFID to bypass a Monotonic Counter protection mechanism. The impact depends on how the anti tear-off feature is used in specific applications such as public transportation, physical access control, etc.	4.2	More Details
CVE-2021-22212	ntpkeygen can generate keys that ntpd fails to parse. NTPsec 1.2.0 allows ntpkeygen to generate keys with '#' characters. ntpd then either pads, shortens the key, or fails to load these keys entirely, depending on the key type and the placement of the '#'. This results in the administrator not being able to use the keys as expected or the keys are shorter than expected and easier to brute-force, possibly resulting in MITM attacks between ntp clients and ntp servers. For short AES128 keys, ntpd generates a warning that it is padding them.	4.0	More Details
CVE-2021-22308	There is a Business Logic Errors vulnerability in Huawei Smartphone. The malicious apps installed on the device can keep taking screenshots in the background. This issue does not cause system errors, but may cause personal information leakage.	3.3	More Details
CVE-2021-23896	Cleartext Transmission of Sensitive Information vulnerability in the administrator interface of McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to view the unencrypted password of the McAfee Insights Server used to pass data to the Insights Server. This user is restricted to only have access to DBSec data in the Insights Server.	3.2	More Details
CVE-2021-22218	All versions of GitLab CE/EE starting from 12.8 before 13.10.5, all versions starting from 13.11 before 13.11.5, and all versions starting from 13.12 before 13.12.2 were affected by an issue in the handling of x509 certificates that could be used to spoof author of signed commits.	2.6	More Details
CVE-2021-33805	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-10906. Reason: This candidate is a duplicate of CVE-2018-10906. Notes: All CVE users should reference CVE-2018-10906 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-26940	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-33500. Reason: This candidate is a reservation duplicate of CVE-2021-33500. Notes: All CVE users should reference CVE-2021-33500 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details