An official website of the United States government Here's how you know

Bulletin (SB21-074)

More Bulletins

Vulnerability Summary for the Week of March 8, 2021

Original release date: March 15, 2021

The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. NVD is sponsored by CISA. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Vulnerabilities are based on the Common Vulnerabilities and Exposures (CVE) vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- High: vulnerabilities with a CVSS base score of 7.0–10.0
- Medium: vulnerabilities with a CVSS base score of 4.0–6.9
- Low: vulnerabilities with a CVSS base score of 0.0–3.9

Entries may include additional information provided by organizations and efforts sponsored by CISA. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletin is compiled from external, open-source reports and is not a direct result of CISA analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to full system compromise.	2021-03-05	9	CVE-2021-26962 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to full system compromise.	2021-03-05	9	CVE-2021-26963 MISC
deutschepost -- mailoptimizer	Deutsche Post Mailoptimizer 4.3 before 2020-11-09 allows Directory Traversal via a crafted ZIP archive to the Upload feature or the MO Connect component. This can lead to remote code execution.	2021-03-05	8.3	CVE-2021-28042 MISC MISC
drweb -- security_space	Dr.Web Security Space versions 11 and 12 allow elevation of privilege for local users without administrative privileges to NT AUTHORITY\SYSTEM due to insufficient control during autoupdate.	2021-03-08	7.2	CVE-2020-23967 MISC MISC MISC
google -- android	In the Citadel chip firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175116439	2021-03-10	7.2	CVE-2021-0455 MISC
google -- android	In the Citadel chip firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117047	2021-03-10	7.2	CVE-2021-0454 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
madge_project -- madge	This affects the package madge before 4.0.1. It is possible to specify a custom Graphviz path via the graphVizPath option parameter which when the .image(), .svg() or .dot() functions are called, is executed by the childprocess.exec function.	2021-03-09	7.5	CVE-2021-23352 MISC MISC MISC
microsoft -- windows_10	Windows Hyper-V Remote Code Execution Vulnerability	2021-03-11	7.2	CVE-2021-26867 MISC
microsoft -- windows_10	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26875, CVE-2021-26900, CVE-2021-27077.	2021-03-11	7.2	CVE-2021-26863 MISC MISC
microsoft -- windows_10	Windows Installer Elevation of Privilege Vulnerability	2021-03-11	7.2	CVE-2021-26862 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26895, CVE-2021-26897.	2021-03-11	10	CVE-2021-26894 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26894, CVE-2021-26895, CVE-2021-26897.	2021-03-11	7.5	CVE-2021-26893 MISC
nano_arena_project -- nano_arena	An issue was discovered in the nano_arena crate before 0.5.2 for Rust. There is an aliasing violation in split_at because two mutable references can exist for the same element, if Borrow<Idx> behaves in certain ways. This can have a resultant out-of-bounds write or use-after-free.	2021-03-05	7.5	CVE-2021-28032 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
newlib_project -- newlib	A flaw was found in newlib in versions prior to 4.0.0. Improper overflow validation in the memory allocation functions mEMALIGn, pvALLOc, nano_memalign, nano_valloc, nano_pvalloc could case an integer overflow, leading to an allocation of a small buffer and then to a heap-based buffer overflow.	2021-03-05	7.5	CVE-2021-3420 MISC FEDORA FEDORA
openbsd -- openssh	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.	2021-03-05	7.5	CVE-2021-28041 MISC MISC MISC MISC
sfcyazilim -- sonlogger	SonLogger before 6.4.1 is affected by Unauthenticated Arbitrary File Upload. An attacker can send a POST request to /Config/SaveUploadedHotspotLogoFile without any authentication or session header. There is no check for the file extension or content of the uploaded file.	2021-03-05	7.5	CVE-2021-27964 MISC MISC
spnego_http_authentication_module_project -- spnego_http_authentication_module	In the SPNEGO HTTP Authentication Module for nginx (spnego-http-auth-nginx-module) before version 1.1.1 basic Authentication can be bypassed using a malformed username. This affects users of spnego-http-auth-nginx-module that have enabled basic authentication. This is fixed in version 1.1.1 of spnego-http-auth-nginx-module. As a workaround, one may disable basic authentication.	2021-03-08	7.5	CVE-2021-21335 MISC MISC CONFIRM
thedaylightstudio -- fuel_cms	FUEL CMS 1.4.8 allows SQL injection via the 'fuel_replace_id' parameter in pages/replace/1. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	2021-03-10	7.5	CVE-2020-24791 MISC MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totvs -- fluig	The TOTVS Fluig platform allows path traversal through the parameter "file = .. /" encoded in base64. This affects all versions Fluig Lake 1.7.0, Fluig 1.6.5 and Fluig 1.6.4	2021-03-05	7.8	CVE-2020-29134 MISC MISC MISC
xmlhttprequest_project -- xmlhttprequest	This affects the package xmlhttprequest before 1.7.0; all versions of package xmlhttprequest-ssl. Provided requests are sent synchronously (async=False on xhr.open), malicious user input flowing into xhr.send could result in arbitrary code being injected and run.	2021-03-05	7.5	CVE-2020-28502 MISC MISC MISC MISC MISC
zohocorp -- manageengine_applications_manager	Zoho ManageEngine Application Control Plus before 100523 has an insecure SSL configuration setting for Nginx, leading to Privilege Escalation.	2021-03-05	7.5	CVE-2020-29658 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
afterlogic -- aurora	An issue was discovered in AfterLogic Aurora through 7.7.9 and WebMail Pro through 7.7.9. They allow directory traversal to read files (such as a data/settings/settings.xml file containing admin panel credentials), as demonstrated by dav/server.php/files/personal/%2e%2e when using the caldav_public_user account (with caldav_public_user as its password).	2021-03-07	5	CVE-2021-26294 MISC
ansi_up_project -- ansi_up	The npm package ansi_up converts ANSI escape codes into HTML. In ansi_up v4, ANSI escape codes can be used to create HTML hyperlinks. Due to insufficient URL sanitization, this feature is affected by a cross-site scripting (XSS) vulnerability. This issue is fixed in v5.0.0.	2021-03-05	4.3	CVE-2021-3377 MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave web-base management interface could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system leading to partial system compromise.	2021-03-05	6.5	CVE-2021-26970 MISC
arubanetworks -- airwave	A remote reflected cross-site scripting (xss) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the web-based management interface of AirWave could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of certain components of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the AirWave management interface.	2021-03-05	4.3	CVE-2021-26967 MISC
arubanetworks -- airwave	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave web-base management interface could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system leading to partial system compromise.	2021-03-05	6.5	CVE-2021-26971 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave	A remote unauthenticated cross-site request forgery (csrf) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an unauthenticated remote attacker to conduct a CSRF attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user.	2021-03-05	6.8	CVE-2021-26961 MISC
arubanetworks -- airwave	A remote unauthenticated cross-site request forgery (csrf) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an unauthenticated remote attacker to conduct a CSRF attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user.	2021-03-05	6.8	CVE-2021-26960 MISC
arubanetworks -- airwave	A remote authentication restriction bypass vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an authenticated remote attacker to improperly access and modify devices and management user details. A successful exploit would consist of an attacker using a lower privileged account to change management user or device details. This could allow the attacker to escalate privileges and/or change network details that they should not have access to.	2021-03-05	5.5	CVE-2021-26964 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave	A remote authenticated sql injection vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Multiple vulnerabilities in the API of AirWave could allow an authenticated remote attacker to conduct SQL injection attacks against the AirWave instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database.	2021-03-05	5.5	CVE-2021-26965 MISC
arubanetworks -- airwave	A remote authenticated sql injection vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Multiple vulnerabilities in the API of AirWave could allow an authenticated remote attacker to conduct SQL injection attacks against the AirWave instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database.	2021-03-05	5.5	CVE-2021-26966 MISC
arubanetworks -- airwave	A remote authenticated authenticated xml external entity (xxe) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Due to improper restrictions on XML entities a vulnerability exists in the web-based management interface of AirWave. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition.	2021-03-05	5.5	CVE-2021-26969 MISC
dell -- emc_powerscale_onefs	PowerScale OneFS 8.1.2,8.2.2 and 9.1.0 contains an improper input sanitization issue in a command. The Compadmin user could potentially exploit this vulnerability, leading to potential privileges escalation.	2021-03-08	4.6	CVE-2021-21503 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- emc_powerscale_onefs	PowerScale OneFS 8.1.2,8.2.2 and 9.1.0 contains an improper input sanitization issue in its API handler. An un-authtenticated with ISI_PRIV_SYS_SUPPORT and ISI_PRIV_LOGIN_PAPI privileges could potentially exploit this vulnerability, leading to potential privileges escalation.	2021-03-08	6.5	CVE-2021-21506 MISC
dell -- idrac8_firmware	Dell iDRAC8 versions prior to 2.75.100.75 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary 'Host' header values to poison a web-cache or trigger redirections.	2021-03-08	5.8	CVE-2021-21510 MISC
elastic -- elasticsearch	A document disclosure flaw was found in Elasticsearch versions after 7.6.0 and before 7.11.0 when Document or Field Level Security is used. Get requests do not properly apply security permissions when executing a query against a recently updated document. This affects documents that have been updated and not yet refreshed in the index. This could result in the search disclosing the existence of documents and fields the attacker should not be able to view.	2021-03-08	4	CVE-2021-22134 MISC
facebook -- react-dev-utils	react-dev-utils prior to v11.0.4 exposes a function, getProcessForPort, where an input argument is concatenated into a command string to be executed. This function is typically used from react-scripts (in Create React App projects), where the usage is safe. Only when this function is manually invoked with user-provided values (ie: by custom code) is there the potential for command injection. If you're consuming it from react-scripts then this issue does not affect you.	2021-03-09	6.8	CVE-2021-24033 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
go-proxyproto_project -- go-proxyproto	The package github.com/pires/go-proxyproto before 0.5.0 are vulnerable to Denial of Service (DoS) via the parseVersion1() function. The reader in this package is a default bufio.Reader wrapping a net.Conn. It will read from the connection until it finds a newline. Since no limits are implemented in the code, a deliberately malformed V1 header could be used to exhaust memory in a server process using this code - and create a DoS. This can be exploited by sending a stream starting with PROXY and continuing to send data (which does not contain a newline) until the target stops acknowledging. The risk here is small, because only trusted sources should be allowed to send proxy protocol headers.	2021-03-08	4	CVE-2021-23351 MISC MISC MISC MISC
google -- android	In deletePackageVersionedInternal of PackageManagerService.java, there is a possible way to exit Screen Pinning due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-135604684	2021-03-10	4.6	CVE-2020-0025 MISC
google -- android	In getMediaOutputSliceAction of RemoteMediaSlice.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174047735	2021-03-10	4.6	CVE-2021-0372 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onReceive of DcTracker.java, there is a possible way to trigger a provisioning URL and modify other telephony settings due to a missing permission check. This could lead to local escalation of privilege during the onboarding flow with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172459128	2021-03-10	4.6	CVE-2021-0380 MISC
google -- android	In createConnectToAvailableNetworkNotification of ConnectToNetworkNotificationBuilder.java, there is a possible connection to untrusted WiFi networks due to notification interaction above the lockscreen. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172584372	2021-03-10	4.6	CVE-2021-0385 MISC
google -- android	In onReceive of ImsPhoneCallTracker.java, there is a possible misattribution of data usage due to an incorrect broadcast handler. This could lead to local escalation of privilege resulting in attributing video call data to the wrong app, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162741489	2021-03-10	4.6	CVE-2021-0388 MISC
google -- android	In setNightModeActivated of UiModeManagerService.java, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168039904	2021-03-10	4.6	CVE-2021-0389 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In main of main.cpp, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-175124730	2021-03-10	4.6	CVE-2021-0392 MISC
google -- android	In StopServicesAndLogViolations of reboot.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-170315126	2021-03-10	4.6	CVE-2021-0395 MISC
google -- android	In getNbits of pvmp3_getbits.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154076193	2021-03-10	4.3	CVE-2021-0378 MISC
google -- android	In getUpTo17bits of pvmp3_getbits.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154075955	2021-03-10	4.3	CVE-2021-0379 MISC
google -- android	In read_and_discard_scanlines of jdapistd.c, there is a possible null pointer exception due to a missing NULL check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173702583	2021-03-10	4.3	CVE-2021-0384 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In done of CaptivePortalLoginActivity.java, there is a confused deputy. This could lead to local escalation of privilege in carrier settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160871056	2021-03-10	4.6	CVE-2021-0383 MISC
google -- android	In FindQuotaDeviceForUuid of QuotaUtils.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169421939	2021-03-10	6.9	CVE-2021-0387 MISC
google -- android	In Scanner::LiteralBuffer::NewCapacity of scanner.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if an attacker can supply a malicious PAC file, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-168041375	2021-03-10	6.8	CVE-2021-0393 MISC
google -- android	In onCreate of UsbConfirmActivity, there is a possible tapjacking vector due to an insecure default value. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173421110	2021-03-10	6.8	CVE-2021-0386 MISC
google -- android	In onCreate() of ChooseTypeAndAccountActivity.java, there is a possible way to learn the existence of an account, without permissions, due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-172841550	2021-03-10	6.8	CVE-2021-0391 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in tab search in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21180 MISC MISC
google -- chrome	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21165 MISC MISC
google -- chrome	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21166 MISC MISC
google -- chrome	Insufficient policy enforcement in Autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21177 MISC MISC
google -- chrome	Inappropriate implementation in full screen mode in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21176 MISC MISC
google -- chrome	Use after free in bookmarks in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21167 MISC MISC
google -- chrome	Inappropriate implementation in Site isolation in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21175 MISC MISC
google -- chrome	Side-channel information leakage in Network Internals in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21173 MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect security UI in TabStrip and Navigation in Google Chrome on Android prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21171 MISC MISC
google -- chrome	Incorrect security UI in Loader in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21170 MISC MISC
google -- chrome	Use after free in WebRTC in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21162 MISC MISC
google -- chrome	Insufficient policy enforcement in appcache in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21168 MISC MISC
google -- chrome	Insufficient data validation in Chrome on iOS in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21164 MISC MISC
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-03-09	6.8	CVE-2021-21190 MISC MISC
google -- chrome	Insufficient data validation in Reader Mode in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page and a malicious server.	2021-03-09	4.3	CVE-2021-21163 MISC MISC
google -- chrome	Out of bounds memory access in V8 in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21169 MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in Referrer in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21174 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21188 MISC MISC
google -- chrome	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21178 MISC MISC
google -- chrome	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21161 MISC MISC
google -- chrome	Use after free in Network Internals in Google Chrome on Linux prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21179 MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 89.0.4389.72 allowed an attacker who convinced a user to install a malicious extension to obtain sensitive information via a crafted Chrome Extension.	2021-03-09	4.3	CVE-2021-21185 MISC MISC
google -- chrome	Heap buffer overflow in WebAudio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21160 MISC MISC
google -- chrome	Insufficient policy enforcement in payments in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21189 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-03-09	6.8	CVE-2021-21159 MISC MISC
google -- chrome	Insufficient data validation in URL formatting in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2021-03-09	4.3	CVE-2021-21187 MISC MISC
google -- chrome	Side-channel information leakage in autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21181 MISC MISC
google -- chrome	Insufficient policy enforcement in QR scanning in Google Chrome on iOS prior to 89.0.4389.72 allowed an attacker who convinced the user to scan a QR code to bypass navigation restrictions via a crafted QR code.	2021-03-09	4.3	CVE-2021-21186 MISC MISC
google -- chrome	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21184 MISC MISC
google -- chrome	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21183 MISC MISC
google -- chrome	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 89.0.4389.72 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	2021-03-09	5.8	CVE-2021-21172 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in navigations in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	2021-03-09	4.3	CVE-2021-21182 MISC MISC
ibm -- api_connect	IBM API Connect V10 and V2018 could allow an attacker who has intercepted a registration invitation link to impersonate the registered user or obtain sensitive information. IBM X-Force ID: 191105.	2021-03-08	6.4	CVE-2020-4903 XF CONFIRM
ibm -- api_connect	IBM API Connect V10 is impacted by insecure communications during database replication. As the data replication happens over insecure communication channels, an attacker can view unencrypted data leading to a loss of confidentiality.	2021-03-08	5	CVE-2020-4695 XF CONFIRM
ibm -- cloud_pak_for_multicloud_management_monitoring	IBM Cloud Pak for Multicloud Management Monitoring 2.2 returns potentially sensitive information in headers which could lead to further attacks against the system. IBM X-Force ID: 194513.	2021-03-09	5	CVE-2021-20341 XF CONFIRM
identitymodel_project -- identitymodel	An issue was discovered in IdentityModel (aka ScottBrady.IdentityModel) before 1.3.0. The Branca implementation allows an attacker to modify and forge authentication tokens.	2021-03-05	5	CVE-2020-36255 MISC MISC MISC
imagemagick -- imagemagick	A flaw was found in ImageMagick in coders/jp2.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	2021-03-09	4.3	CVE-2021-20241 MISC MISC
imagemagick -- imagemagick	A flaw was found in ImageMagick in MagickCore/resize.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	2021-03-09	4.3	CVE-2021-20243 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inetsoftware -- i-net_clear_reports	I-Net Software Clear Reports 20.10.136 web application accepts a user-controlled input that specifies a link to an external site, and uses the user supplied data in a Redirect.	2021-03-09	5.8	CVE-2020-28150 MISC
jpeg -- jpeg-xl	jpeg-xl v0.3.2 is affected by a heap buffer overflow in /lib/jxl/coeff_order.cc ReadPermutation. When decoding a malicous jxl file using djxl, an attacker can trigger arbitrary code execution or a denial of service.	2021-03-05	6.8	CVE-2021-28026 MISC
libtiff -- libtiff	In LibTIFF, there is a memory malloc failure in tif_pixarlog.c. A crafted TIFF document can lead to an abort, resulting in a remote denial of service attack.	2021-03-09	4.3	CVE-2020-35522 MISC
libtiff -- libtiff	A flaw was found in libtiff. Due to a memory allocation failure in tif_read.c, a crafted TIFF file can lead to an abort, resulting in denial of service.	2021-03-09	4.3	CVE-2020-35521 MISC
linux -- linux_kernel	A flaw was found in the Linux kernel in versions prior to 5.10. A violation of memory access was found while detecting a padding of int3 in the linking state. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-03-09	4.6	CVE-2021-3411 MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks necessary treatment of errors such as failed memory allocations (as a result of changes to the handling of grant mapping errors). A host OS denial of service may occur during misbehavior of a networking frontend driver. NOTE: this issue exists because of an incomplete fix for CVE-2021-26931.	2021-03-05	4.9	CVE-2021-28038 MLIST MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mantisbt -- mantisbt	An issue was discovered in MantisBT before 2.24.5. It associates a unique cookie string with each user. This string is not reset upon logout (i.e., the user session is still considered valid and active), allowing an attacker who somehow gained access to a user's cookie to login as them.	2021-03-07	5.5	CVE-2009-20001 MISC MISC
maxum -- rumpus	Maxum Rumpus 8.2.13 and 8.2.14 is affected by cross-site request forgery (CSRF). If an authenticated user visits a malicious page, unintended actions could be performed in the web application as the authenticated user.	2021-03-08	6.8	CVE-2020-27574 MISC MISC
maxum -- rumpus	Maxum Rumpus 8.2.13 and 8.2.14 is affected by a command injection vulnerability. The web administration contains functionality in which administrators are able to manage users. The edit users form contains a parameter vulnerable to command injection due to insufficient validation.	2021-03-08	6.5	CVE-2020-27575 MISC MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-24089 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-24110 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-26902 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-27047 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-27048 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-27049 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-27051 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27061.	2021-03-11	6.8	CVE-2021-27062 MISC
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27050, CVE-2021-27051, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-27061 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- high_efficiency_video_coding	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24089, CVE-2021-24110, CVE-2021-26902, CVE-2021-27047, CVE-2021-27048, CVE-2021-27049, CVE-2021-27051, CVE-2021-27061, CVE-2021-27062.	2021-03-11	6.8	CVE-2021-27050 MISC
microsoft -- windows_10	Windows Container Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26865.	2021-03-11	4.6	CVE-2021-26891 MISC
microsoft -- windows_10	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1640.	2021-03-11	4.6	CVE-2021-26878 MISC
microsoft -- windows_10	Application Virtualization Remote Code Execution Vulnerability	2021-03-11	4.6	CVE-2021-26890 MISC
microsoft -- windows_10	Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability	2021-03-11	4.6	CVE-2021-26887 MISC
microsoft -- windows_10	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	2021-03-11	6.5	CVE-2021-26881 MISC
microsoft -- windows_10	Windows Update Stack Elevation of Privilege Vulnerability	2021-03-11	4.6	CVE-2021-26889 MISC
microsoft -- windows_10	Windows WalletService Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26871.	2021-03-11	4.6	CVE-2021-26885 MISC
microsoft -- windows_10	Remote Access API Elevation of Privilege Vulnerability	2021-03-11	4.6	CVE-2021-26882 MISC
microsoft -- windows_10	Storage Spaces Controller Elevation of Privilege Vulnerability	2021-03-11	4.6	CVE-2021-26880 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Update Service Elevation of Privilege Vulnerability	2021-03-11	4.6	CVE-2021-26866 MISC
microsoft -- windows_10	Windows Container Execution Agent Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26891.	2021-03-11	4.6	CVE-2021-26865 MISC
microsoft -- windows_10	Windows Virtual Registry Provider Elevation of Privilege Vulnerability	2021-03-11	4.6	CVE-2021-26864 MISC
microsoft -- windows_10	Windows NAT Denial of Service Vulnerability	2021-03-11	5	CVE-2021-26879 MISC
microsoft -- windows_10	Windows Graphics Component Remote Code Execution Vulnerability	2021-03-11	6.8	CVE-2021-26861 MISC
minio -- minio	MinIO is an open-source high performance object storage service and it is API compatible with Amazon S3 cloud storage service. In MinIO before version RELEASE.2021-03-04T00-53-13Z it is possible to bypass a readOnly policy by creating a temporary 'mc share upload' URL. Everyone is impacted who uses MinIO multi-users. This is fixed in version RELEASE.2021-03-04T00-53-13Z. As a workaround, one can disable uploads with `Content-Type: multipart/form-data` as mentioned in the S3 API RESTObjectPOST docs by using a proxy in front of MinIO.	2021-03-08	4	CVE-2021-21362 MISC MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- pollbot	Pollbot is open source software which "frees its human masters from the toilsome task of polling for the state of things during the Firefox release process." In Pollbot before version 1.4.4 there is an open redirection vulnerability in the path of "https://pollbot.services.mozilla.com/". An attacker can redirect anyone to malicious sites. To Reproduce type in this URL: "https://pollbot.services.mozilla.com//evil.com/". Affected versions will redirect to that website when you inject a payload like "//evil.com/". This is fixed in version 1.4.4.	2021-03-08	5.8	CVE-2021-21354 MISC MISC MISC MISC MISC CONFIRM
nats -- nats_server	This affects all versions of package github.com/nats-io/nats-server/server. Untrusted accounts are able to crash the server using configs that represent a service export/import cycles. Disclaimer from the maintainers: Running a NATS service which is exposed to untrusted users presents a heightened risk. Any remote execution flaw or equivalent seriousness, or denial-of-service by unauthenticated users, will lead to prompt releases by the NATS maintainers. Fixes for denial of service issues with no threat of remote execution, when limited to account holders, are likely to just be committed to the main development branch with no special attention. Those who are running such services are encouraged to build regularly from git.	2021-03-07	5	CVE-2020-28466 MISC MISC
oryx-embedded -- cyclonetcp	Oryx Embedded CycloneTCP 1.7.6 to 2.0.0, fixed in 2.0.2, is affected by incorrect input validation, which may cause a denial of service (DoS). To exploit the vulnerability, an attacker needs to have TCP connectivity to the target system. Receiving a maliciously crafted TCP packet from an unauthenticated endpoint is sufficient to trigger the bug.	2021-03-08	5	CVE-2021-26788 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ossec -- ossec	An issue was discovered in OSSEC 3.6.0. An uncontrolled recursion vulnerability in os_xml.c occurs when a large number of opening and closing XML tags is used. Because recursion is used in _ReadElem without restriction, an attacker can trigger a segmentation fault once unmapped memory is reached.	2021-03-05	5	CVE-2021-28040 MISC
ougc_feedback_project -- ougc_feedback	The OUGC Feedback plugin before 1.8.23 for MyBB allows XSS via the comment field of feedback during an edit operation.	2021-03-09	4.3	CVE-2021-28115 MISC MISC
privoxy -- privoxy	A flaw was found in privoxy before 3.0.32. A invalid read of size two may occur in chunked_body_is_complete() leading to denial of service.	2021-03-09	5	CVE-2021-20275 MISC MLIST MISC
privoxy -- privoxy	A flaw was found in privoxy before 3.0.32. A crash may occur due a NULL-pointer dereference when the socks server misbehaves.	2021-03-09	5	CVE-2021-20274 MISC MISC
privoxy -- privoxy	A flaw was found in privoxy before 3.0.32. A crash can occur via a crafted CGI request if Privoxy is toggled off.	2021-03-09	5	CVE-2021-20273 MISC MLIST MISC
privoxy -- privoxy	A flaw was found in privoxy before 3.0.32. An assertion failure could be triggered with a crafted CGI request leading to server crash.	2021-03-09	5	CVE-2021-20272 MISC MLIST MISC
privoxy -- privoxy	A flaw was found in privoxy before 3.0.32. Invalid memory access with an invalid pattern passed to pcre_compile() may lead to denial of service.	2021-03-09	5	CVE-2021-20276 MISC MLIST MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rancher -- rancher	A Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rancher allows remote attackers to execute JavaScript via malicious links. This issue affects: SUSE Rancher Rancher versions prior to 2.5.6.	2021-03-05	4.3	CVE-2021-25313 CONFIRM CONFIRM CONFIRM
ratcf -- ratcf	RATCF is an open-source framework for hosting Cyber-Security Capture the Flag events. In affected versions of RATCF users with multi factor authentication enabled are able to log in without a valid token. This is fixed in commit cebb67b.	2021-03-08	6.8	CVE-2021-21329 MISC MISC CONFIRM
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Universal 3D (.U3D) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27592 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Portable Document Format (.PDF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27591 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Tag Image File Format (.TIFF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27590 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Scalable Vector Graphics (.SVG) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27589 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated HPGL format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27588 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Jupiter Tessellation (.JT) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27587 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Interchange File Format (.IFF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27586 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Computer Graphics Metafile (.CGM) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27585 MISC MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated PhotoShop Document (.PSD) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	4.3	CVE-2021-27584 MISC MISC
secomea -- gatemanager_8250_firmware	Upload of Code Without Integrity Check vulnerability in firmware archive of Secomea GateManager allows authenticated attacker to execute malicious code on server. This issue affects: Secomea GateManager all versions prior to 9.4.621054022	2021-03-05	6.5	CVE-2020-29032 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
secomea -- gatemanager_firmware	Cross-site Scripting (XSS) vulnerability in web GUI of Secomea GateManager allows an attacker to inject arbitrary javascript code. This issue affects: Secomea GateManager all versions prior to 9.4.	2021-03-05	4.3	CVE-2020-29028 MISC
secomea -- gatemanager_firmware	Cross-Site Request Forgery (CSRF) vulnerability in web GUI of Secomea GateManager allows an attacker to execute malicious code. This issue affects: Secomea GateManager All versions prior to 9.4.	2021-03-05	6.8	CVE-2020-29030 MISC
secomea -- gatemanager_firmware	Improper Input Validation, Cross-site Scripting (XSS) vulnerability in Web GUI of Secomea GateManager allows an attacker to execute arbitrary javascript code. This issue affects: Secomea GateManager all versions prior to 9.4.	2021-03-05	4.3	CVE-2020-29029 MISC
secomea -- sitemanager_firmware	Improper Access Control vulnerability in web service of Secomea SiteManager allows remote attacker to access the web UI from the internet using the configured credentials. This issue affects: Secomea SiteManager All versions prior to 9.4.620527004 on Hardware.	2021-03-05	6.5	CVE-2020-29020 MISC
sfcyazilim -- sonlogger	SonLogger before 6.4.1 is affected by user creation with any user permissions profile (e.g., SuperAdmin). An anonymous user can send a POST request to /User/saveUser without any authentication or session header.	2021-03-05	6.4	CVE-2021-27963 MISC MISC
squarebox -- catdv	An issue was discovered in SquareBox CatDV Server through 9.2. An attacker can invoke sensitive RMI methods such as getConnections without authentication, the results of which can be used to generate valid authentication tokens. These tokens can then be used to invoke administrative tasks within the application, such as disclosing password hashes.	2021-03-05	6.4	CVE-2021-26705 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
squid-cache -- squid	Squid through 4.14 and 5.x through 5.0.5, in some configurations, allows information disclosure because of an out-of-bounds read in WCCP protocol data. This can be leveraged as part of a chain for remote code execution as nobody.	2021-03-09	4.3	CVE-2021-28116 MISC MISC MISC
thedaylightstudio -- fuel_cms	An issue was discovered in FUEL CMS 1.4.7. There is a escalation of privilege vulnerability to obtain super admin privilege via the "id" and "fuel_id" parameters.	2021-03-10	6.5	CVE-2020-23722 MISC
thedaylightstudio -- fuel_cms	FUEL CMS 1.4.13 contains a cross-site request forgery (CSRF) vulnerability that can delete a page via a post ID to /pages/delete/3.	2021-03-10	4.3	CVE-2020-28705 MISC MISC
wazuh -- wazuh	Wazuh API in Wazuh from 4.0.0 to 4.0.3 allows authenticated users to execute arbitrary code with administrative privileges via /manager/files URI. An authenticated user to the service may exploit incomplete input validation on the /manager/files API to inject arbitrary code within the API service script.	2021-03-06	6.5	CVE-2021-26814 MISC MISC
web_based_quiz_system_project -- web_based_quiz_system	Web Based Quiz System 1.0 is affected by cross-site scripting (XSS) in admin.php through the options parameter.	2021-03-09	4.3	CVE-2021-28006 MISC
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus before 7066 allows XSS.	2021-03-05	4.3	CVE-2020-35594 MISC
zohocorp -- manageengine_desktop_central	Zoho ManageEngine Desktop Central before build 10.0.647 allows a single authentication secret from multiple agents to communicate with the server.	2021-03-05	6.4	CVE-2020-28050 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zope -- products.genericsetup	Products.GenericSetup is a mini-framework for expressing the configured state of a Zope Site as a set of filesystem artifacts. In Products.GenericSetup before version 2.1.1 there is an information disclosure vulnerability - anonymous visitors may view log and snapshot files generated by the Generic Setup Tool. The problem has been fixed in version 2.1.1. Depending on how you have installed Products.GenericSetup, you should change the buildout version pin to 2.1.1 and re-run the buildout, or if you used pip simply do pip install `"Products.GenericSetup>=2.1.1"`.	2021-03-09	5	CVE-2021-21360 MISC CONFIRM MISC
zope -- products.pluggableauthservice	Products.PluggableAuthService is a pluggable Zope authentication and authorization framework. In Products.PluggableAuthService before version 2.6.0 there is an information disclosure vulnerability - everyone can list the names of roles defined in the ZODB Role Manager plugin if the site uses this plugin. The problem has been fixed in version 2.6.0. Depending on how you have installed Products.PluggableAuthService, you should change the buildout version pin to 2.6.0 and re-run the buildout, or if you used pip simply do `pip install "Products.PluggableAuthService>=2.6.0"`.	2021-03-08	4	CVE-2021-21336 MISC CONFIRM MISC
zope -- products.pluggableauthservice	Products.PluggableAuthService is a pluggable Zope authentication and authorization framework. In Products.PluggableAuthService before version 2.6.0 there is an open redirect vulnerability. A maliciously crafted link to the login form and login functionality could redirect the browser to a different website. The problem has been fixed in version 2.6.1. Depending on how you have installed Products.PluggableAuthService, you should change the buildout version pin to `2.6.1` and re-run the buildout, or if you used `pip` simply do `pip install "Products.PluggableAuthService>=2.6.1".	2021-03-08	5.8	CVE-2021-21337 MISC CONFIRM MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- oozie	There is a race condition in OozieSharelibCLI in Apache Oozie before version 5.2.1 which allows a malicious attacker to replace the files in Oozie's sharelib during it's creation.	2021-03-09	1.9	CVE-2020-35451 MLIST MISC MLIST
apache -- superset	Apache Superset up to and including 0.38.0 allowed the creation of a Markdown component on a Dashboard page for describing chart's related information. Abusing this functionality, a malicious user could inject javascript code executing unwanted action in the context of the user's browser. The javascript code will be automatically executed (Stored XSS) when a legitimate user surfs on the dashboard page. The vulnerability is exploitable creating a “div” section and embedding in it a “svg” element with javascript code.	2021-03-05	3.5	CVE-2021-27907 MISC MLIST
arubanetworks -- airwave	A remote authenticated stored cross-site scripting (xss) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the web-based management interface of AirWave could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim’s browser in the context of the affected interface.	2021-03-05	3.5	CVE-2021-26968 MISC
batflat -- batflat	Cross-site scripting (XSS) vulnerability in Galleries in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name.	2021-03-11	3.5	CVE-2021-27677 MISC
batflat -- batflat	Cross-site scripting (XSS) vulnerability in Snippets in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name.	2021-03-11	3.5	CVE-2021-27678 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
batflat -- batflat	Cross-site scripting (XSS) vulnerability in Navigation in Batflat CMS 1.3.6 allows remote attackers to inject arbitrary web script or HTML via the field name.	2021-03-11	3.5	CVE-2021-27679 MISC
cszcms -- csz_cms	A stored cross-site scripting (XSS) vulnerability in cszcms 1.2.9 exists in /admin/pages/new via the content parameter.	2021-03-10	3.5	CVE-2021-3224 MISC MISC
google -- android	In checkSlicePermission of SliceManagerService.java, there is a possible resource exposure due to an incorrect permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140727941	2021-03-10	2.1	CVE-2021-0382 MISC
google -- android	In the Titan-M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117199	2021-03-10	2.1	CVE-2021-0453 MISC
google -- android	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117261	2021-03-10	2.1	CVE-2021-0452 MISC
google -- android	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117871	2021-03-10	2.1	CVE-2021-0451 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117880	2021-03-10	2.1	CVE-2021-0450 MISC
google -- android	In the Titan M chip firmware, there is a possible disclosure of stack memory due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175117965	2021-03-10	2.1	CVE-2021-0449 MISC
google -- android	In android_os_Parcel_readString8 of android_os_Parcel.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-172655291	2021-03-10	2.1	CVE-2021-0394 MISC
google -- android	In onPackageModified of VoiceInteractionManagerService.java, there is a possible change of default applications due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-167261484	2021-03-10	2.1	CVE-2021-0375 MISC
google -- android	In updateNotifications of DeviceStorageMonitorService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153466381	2021-03-10	2.1	CVE-2021-0381 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In BnAudioPolicyService::onTransact of IAudioPolicyService.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169572641	2021-03-10	2.1	CVE-2021-0374 MISC
impresscms -- impresscms	Cross-site scripting (XSS) in modules/content/admin/content.php in ImpressCMS profile 1.4.2 allows remote attackers to inject arbitrary web script or HTML parameters through the "Display Name" field.	2021-03-11	3.5	CVE-2021-28088 MISC MISC
lenovo -- pcmanager	A denial of service vulnerability was reported in Lenovo PCManager, prior to version 3.0.200.2042, that could allow configuration files to be written to non-standard locations.	2021-03-09	2.1	CVE-2020-8357 MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel 5.9.x through 5.11.3, as used with Xen. In some less-common configurations, an x86 PV guest OS user can crash a Dom0 or driver domain via a large amount of I/O activity. The issue relates to misuse of guest physical addresses when a configuration has CONFIG_XEN_UNPOPULATED_ALLOC but not CONFIG_XEN_BALLOON_MEMORY_HOTPLUG.	2021-03-05	2.1	CVE-2021-28039 MLIST MISC
maxum -- rumpus	Maxum Rumpus 8.2.13 and 8.2.14 is affected by cross-site scripting (XSS). Users are able to create folders in the web application. The folder name is insufficiently validated resulting in a stored cross-site scripting vulnerability.	2021-03-08	3.5	CVE-2020-27576 MISC MISC
microsoft -- windows_10	Windows Media Photo Codec Information Disclosure Vulnerability	2021-03-11	2.1	CVE-2021-26884 MISC
microsoft -- windows_10	User Profile Service Denial of Service Vulnerability	2021-03-11	2.1	CVE-2021-26886 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability	2021-03-11	2.1	CVE-2021-26892 MISC
obss -- time_in_status	In the "Time in Status" app before 4.13.0 for Jira, remote authenticated attackers can cause Stored XSS.	2021-03-08	3.5	CVE-2021-27222 MISC MISC MISC
thedaylightstudio -- fuel_cms	An issue was discovered in FUEL CMS V1.4.7. An attacker can use a XSS payload and bypass a filter via /fuelCM/fuel/pages/edit/1?lang=english.	2021-03-10	3.5	CVE-2020-23721 MISC
zte -- zxhn_h196q_firmware	A ZTE product has an information leak vulnerability. An attacker with higher authority can go beyond their authority to access files in other directories by performing specific operations, resulting in information leak. This affects: ZXHN H196Q V9.1.0C2.	2021-03-05	2.7	CVE-2021-21725 MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	Windows App-V Overlay Filter Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-26860 MISC
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21077 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21074 MISC
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21075 MISC
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21076 MISC
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by a Memory Corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21071 MISC
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21072 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- animate	Adobe Animate version 21.0.3 (and earlier) is affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21073 MISC
adobe -- connect	Adobe Connect version 11.0.7 (and earlier) is affected by an Input Validation vulnerability in the export feature. An attacker could exploit this vulnerability by injecting a payload into the registration form and achieve arbitrary code execution in the context of the admin account.	2021-03-12	not yet calculated	CVE-2021-21085 MISC
adobe -- connect	Adobe Connect version 11.0.7 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious JavaScript content that may be executed within the context of the victim's browser when they browse to the page containing the vulnerable field.	2021-03-12	not yet calculated	CVE-2021-21080 MISC
adobe -- connect	Adobe Connect version 11.0.7 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious JavaScript content that may be executed within the context of the victim's browser when they browse to the page containing the vulnerable field.	2021-03-12	not yet calculated	CVE-2021-21079 MISC
adobe -- creative_cloud_desktop_application	Adobe Creative Cloud Desktop Application version 5.3 (and earlier) is affected by a local privilege escalation vulnerability that could allow an attacker to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction.	2021-03-12	not yet calculated	CVE-2021-21069 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- creative_cloud_desktop_application	Adobe Creative Cloud Desktop Application version 5.3 (and earlier) is affected by a file handling vulnerability that could allow an attacker to cause arbitrary file overwriting. Exploitation of this issue requires physical access and user interaction.	2021-03-12	not yet calculated	CVE-2021-21068 MISC
adobe -- creative_cloud_desktop_application	Adobe Creative Cloud Desktop Application version 5.3 (and earlier) is affected by an Unquoted Service Path vulnerability in CCXProcess that could allow an attacker to achieve arbitrary code execution in the process of the current user. Exploitation of this issue requires user interaction	2021-03-12	not yet calculated	CVE-2021-21078 MISC
adobe -- framemaker	Adobe Framemaker version 2020.0.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21056 MISC
adobe -- photoshop	Adobe Photoshop versions 21.2.5 (and earlier) and 22.2 (and earlier) are affected by a Memory Corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21082 MISC
adobe -- photoshop	Adobe Photoshop versions 21.2.5 (and earlier) and 22.2 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-03-12	not yet calculated	CVE-2021-21067 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ansible-tower -- ansible-tower	A flaw was found in ansible-tower. The default installation is vulnerable to Job Isolation escape allowing an attacker to elevate the privilege from a low privileged user to the awx user from outside the isolated environment. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-03-09	not yet calculated	CVE-2021-20253 MISC
apache -- velocity	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.	2021-03-10	not yet calculated	CVE-2020-13936 MLIST CONFIRM MLIST MLIST MLIST
apache -- velocity_tools	The default error page for VelocityView in Apache Velocity Tools prior to 3.1 reflects back the vm file that was entered as part of the URL. An attacker can set an XSS payload file as this vm file in the URL which results in this payload being executed. XSS vulnerabilities allow attackers to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.	2021-03-10	not yet calculated	CVE-2020-13959 MLIST CONFIRM MLIST MLIST MLIST
athom -- homey_and_homey_pro_devices	An issue was discovered on Athom Homey and Homey Pro devices before 5.0.0. ZigBee hub devices should generate a unique Standard Network Key that is then exchanged with all enrolled devices so that all inter-device communication is encrypted. However, the vitec Athom products use another widely known key that is designed for testing purposes: "01030507090b0d0f00020406080a0c0d" (the decimal equivalent of 1 3 5 7 9 11 13 15 0 2 4 6 8 10 12 13), which is human generated and static across all issued devices.	2021-03-09	not yet calculated	CVE-2020-28952 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
baby_care_system -- baby_care_system	Baby Care System 1.0 is affected by a cross-site scripting (XSS) vulnerability in the Edit Page tab through the Post title parameter.	2021-03-10	not yet calculated	CVE-2020-35752 MISC MISC MISC
bloomreach -- experience_manager	An issue was discovered in Bloomreach Experience Manager (brXM) 4.1.0 through 14.2.2. It allows remote attackers to execute arbitrary code because there is a mishandling of the capability for administrators to write and run Groovy scripts within the updater editor. An attacker must use an AST transforming annotation such as @Grab.	2021-03-11	not yet calculated	CVE-2020-14987 MISC
bloomreach -- experience_manager	An issue was discovered in Bloomreach Experience Manager (brXM) 4.1.0 through 14.2.2. It allows XSS in the login page via the loginmessage parameter, the text editor via the src attribute of HTML elements, the translations menu via the foldername parameter, the author page via the link URL, or the upload image functionality via an SVG document containing JavaScript.	2021-03-11	not yet calculated	CVE-2020-14988 MISC
bloomreach -- experience_manager	An issue was discovered in Bloomreach Experience Manager (brXM) 4.1.0 through 14.2.2. It allows CSRF if the attacker uses GET where POST was intended.	2021-03-11	not yet calculated	CVE-2020-14989 MISC
camunda -- modeler	** DISPUTED ** Camunda Modeler (aka camunda-modeler) through 4.6.0 allows arbitrary file access. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which manipulates the readFile and writeFile APIs. NOTE: the vendor states "The way we secured the app is that it does not allow any remote scripts to be opened, no unsafe scripts to be evaluated, no remote sites to be browsed."	2021-03-11	not yet calculated	CVE-2021-28154 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
changeset -- changeset	Prototype pollution vulnerability in 'changeset' versions 0.0.1 through 0.2.5 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-03-09	not yet calculated	CVE-2021-25915 MISC MISC
clipper -- clipper	Clipper before 1.0.5 allows remote command execution. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which invokes the dangerous openExternal API.	2021-03-11	not yet calculated	CVE-2021-28134 MISC MISC MISC MISC
com.bmuschko -- com.bmuschko	The `com.bmuschko:gradle-vagrant-plugin` Gradle plugin contains an information disclosure vulnerability due to the logging of the system environment variables. When this Gradle plugin is executed in public CI/CD, this can lead to sensitive credentials being exposed to malicious actors. This is fixed in version 3.0.0.	2021-03-09	not yet calculated	CVE-2021-21361 MISC MISC MISC CONFIRM
containerd -- containerd	In containerd (an industry-standard container runtime) before versions 1.3.10 and 1.4.4, containers launched through containerd's CRI implementation (through Kubernetes, crictl, or any other pod/container client that uses the containerd CRI service) that share the same image may receive incorrect environment variables, including values that are defined for other containers. If the affected containers have different security contexts, this may allow sensitive information to be unintentionally shared. If you are not using containerd's CRI implementation (through one of the mechanisms described above), you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image which have different environment variables, you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image in rapid succession, you have reduced likelihood of being vulnerable to this issue This vulnerability has been fixed in containerd 1.3.10 and containerd 1.4.4. Users should update to these versions.	2021-03-10	not yet calculated	CVE-2021-21334 MISC MISC MISC CONFIRM FEDORA FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cortex -- xsoar	An information exposure through log file vulnerability exists in Cortex XSOAR software where the secrets configured for the SAML single sign-on (SSO) integration can be logged to the '/var/log/demisto/' server logs when testing the integration during setup. This logged information includes the private key and identity provider certificate used to configure the SAML SSO integration. This issue impacts: Cortex XSOAR 5.5.0 builds earlier than 98622; Cortex XSOAR 6.0.1 builds earlier than 830029; Cortex XSOAR 6.0.2 builds earlier than 98623; Cortex XSOAR 6.1.0 builds earlier than 848144.	2021-03-10	not yet calculated	CVE-2021-3034 CONFIRM
csz -- csz	CSZ CMS 1.2.9 is affected by a cross-site scripting (XSS) vulnerability in multiple pages through the field name.	2021-03-11	not yet calculated	CVE-2021-26776 MISC
d-link -- dir-3060_devices	prog.cgi on D-Link DIR-3060 devices before 1.11b04 HF2 allows remote authenticated users to inject arbitrary commands in an admin or root context because SetVirtualServerSettings calls CheckArpTables, which calls popen unsafely.	2021-03-11	not yet calculated	CVE-2021-28144 MISC FULLDISC CONFIRM MISC
d-link-- dir-841_devices	/jsonrpc on D-Link DIR-841 3.03 and 3.04 devices allows authenticated command injection via ping, ping6, or traceroute (under System Tools).	2021-03-11	not yet calculated	CVE-2021-28143 MISC MISC
dell -- supportassist	Dell SupportAssist Client for Consumer PCs versions 3.7.x, 3.6.x, 3.4.x, 3.3.x, Dell SupportAssist Client for Business PCs versions 2.0.x, 2.1.x, 2.2.x, and Dell SupportAssist Client ProManage 1.x contain a DLL injection vulnerability in the Costura Fody plugin. A local user with low privileges could potentially exploit this vulnerability, leading to the execution of arbitrary executable on the operating system with SYSTEM privileges.	2021-03-12	not yet calculated	CVE-2021-21518 CONFIRM

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eclipse -- platform	In versions 4.18 and earlier of the Eclipse Platform, the Help Subsystem does not authenticate active help requests to the local help web server, allowing an unauthenticated local attacker to issue active help commands to the associated Eclipse Platform process or Eclipse Rich Client Platform process.	2021-03-09	not yet calculated	CVE-2020-27225 CONFIRM
eclipse -- theia	In Eclipse Theia versions up to and including 1.8.0, in the debug console there is no HTML escaping, so arbitrary Javascript code can be injected.	2021-03-12	not yet calculated	CVE-2021-28161 CONFIRM
eclipse -- theia	In Eclipse Theia versions up to and including 0.16.0, in the notification messages there is no HTML escaping, so Javascript code can run.	2021-03-12	not yet calculated	CVE-2021-28162 CONFIRM
emerson -- smart_wireless_gateway	Incorrect Access Control in Emerson Smart Wireless Gateway 1420 4.6.59 allows remote attackers to obtain sensitive device information from the administrator console without authentication.	2021-03-10	not yet calculated	CVE-2020-19419 MISC
emerson -- smart_wireless_gateway	Emerson Smart Wireless Gateway 1420 4.6.59 allows non-privileged users (such as the default account 'maint') to perform administrative tasks by sending specially crafted HTTP requests to the application.	2021-03-10	not yet calculated	CVE-2020-19417 MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
envoy -- envoy	Envoy is a cloud-native high-performance edge/middle/service proxy. In Envoy version 1.17.0 an attacker can bypass authentication by presenting a JWT token with an issuer that is not in the provider list when Envoy's JWT Authentication filter is configured with the `allow_missing` requirement under `requires_any` due to a mistake in implementation. Envoy's JWT Authentication filter can be configured with the `allow_missing` requirement that will be satisfied if JWT is missing (JwtMissed error) and fail if JWT is presented or invalid. Due to a mistake in implementation, a JwtUnknownIssuer error was mistakenly converted to JwtMissed when `requires_any` was configured. So if `allow_missing` was configured under `requires_any`, an attacker can bypass authentication by presenting a JWT token with an issuer that is not in the provider list. Integrity may be impacted depending on configuration if the JWT token is used to protect against writes or modifications. This regression was introduced on 2020/11/12 in PR 13839 which fixed handling `allow_missing` under RequiresAny in a JwtRequirement (see issue 13458). The AnyVerifier aggregates the children verifiers' results into a final status where JwtMissing is the default error. However, a JwtUnknownIssuer was mistakenly treated the same as a JwtMissing error and the resulting final aggregation was the default JwtMissing. As a result, `allow_missing` would allow a JWT token with an unknown issuer status. This is fixed in version 1.17.1 by PR 15194. The fix works by preferring JwtUnknownIssuer over a JwtMissing error, fixing the accidental conversion and bypass with `allow_missing`. A user could detect whether a bypass occurred if they have Envoy logs enabled with debug verbosity. Users can enable component level debug logs for JWT. The JWT filter logs will indicate that there is a request with a JWT token and a failure that the JWT token is missing.	2021-03-11	not yet calculated	CVE-2021-21378 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
facebook -- gameroom	The fbgames protocol handler registered as part of Facebook Gameroom does not properly quote arguments passed to the executable. That allows a malicious URL to cause code execution. This issue affects versions prior to v1.26.0.	2021-03-10	not yet calculated	CVE-2021-24030 CONFIRM
flatpak -- flatpak	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In Flatpack since version 0.9.4 and before version 1.10.2 has a vulnerability in the "file forwarding" feature which can be used by an attacker to gain access to files that would not ordinarily be allowed by the app's permissions. By putting the special tokens `@@` and/or `@@u` in the Exec field of a Flatpak app's .desktop file, a malicious app publisher can trick flatpak into behaving as though the user had chosen to open a target file with their Flatpak app, which automatically makes that file available to the Flatpak app. This is fixed in version 1.10.2. A minimal solution is the first commit "`Disallow @@ and @@U usage in desktop files`". The follow-up commits "`dir: Reserve the whole @@ prefix`" and "`dir: Refuse to export .desktop files with suspicious uses of @@ tokens`" are recommended, but not strictly required. As a workaround, avoid installing Flatpak apps from untrusted sources, or check the contents of the exported `.desktop` files in `exports/share/applications/*.desktop` (typically `~/.local/share/flatpak/exports/share/applications/*.desktop` and `/var/lib/flatpak/exports/share/applications/*.desktop`) to make sure that literal filenames do not follow `@@` or `@@u`.	2021-03-11	not yet calculated	CVE-2021-21381 MISC MISC MISC MISC MISC CONFIRM DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
git -- git	Git is an open-source distributed revision control system. In affected versions of Git a specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS+ or APFS (i.e. the default file systems on Windows and macOS). Note that clean/smudge filters have to be configured for that. Git for Windows configures Git LFS by default, and is therefore vulnerable. The problem has been patched in the versions published on Tuesday, March 9th, 2021. As a workaound, if symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. _before_ cloning), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14.2. The fix versions are: 2.30.1, 2.29.3, 2.28.1, 2.27.1, 2.26.3, 2.25.5, 2.24.4, 2.23.4, 2.22.5, 2.21.4, 2.20.5, 2.19.6, 2.18.5, 2.17.62.17.6.	2021-03-09	not yet calculated	CVE-2021-21300 MLIST MISC CONFIRM MISC MISC FEDORA MISC
glpi -- glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 it is possible to create tickets for another user with self-service interface without delegatee systems enabled. This is fixed in version 9.5.4.	2021-03-08	not yet calculated	CVE-2021-21326 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi -- glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 there is an Insecure Direct Object Reference (IDOR) on "Solutions". This vulnerability gives an unauthorized user the ability to enumerate GLPI items names (including users logins) using the knowbase search form (requires authentication). To Reproduce: Perform a valid authentication at your GLPI instance, Browse the ticket list and select any open ticket, click on Solution form, then Search a solution form that will redirect you to the endpoint /"glpi/front/knowbaseitem.php?item_itemtype=Ticket&item_items_id=18&forcetab=Knowbase$1", and the item_itemtype=Ticket parameter present in the previous URL will point to the PHP alias of glpi_tickets table, so just replace it with "Users" to point to glpi_users table instead; in the same way, item_items_id=18 will point to the related column id, so changing it too you should be able to enumerate all the content which has an alias. Since such id(s) are obviously incremental, a malicious party could exploit the vulnerability simply by guessing-based attempts.	2021-03-08	not yet calculated	CVE-2021-21324 MISC MISC CONFIRM
glpi -- glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 non-authenticated user can remotely instantiate object of any class existing in the GLPI environment that can be used to carry out malicious attacks, or to start a “POP chain”. As an example of direct impact, this vulnerability affects integrity of the GLPI core platform and third-party plugins runtime misusing classes which implement some sensitive operations in their constructors or destructors. This is fixed in version 9.5.4.	2021-03-08	not yet calculated	CVE-2021-21327 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi -- glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 a new budget type can be defined by user. This input is not correctly filtered. This results in a cross-site scripting attack. To exploit this endpoint attacker need to be authenticated. This is fixed in version 9.5.4.	2021-03-08	not yet calculated	CVE-2021-21325 MISC CONFIRM
gnome -- glib	An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)	2021-03-11	not yet calculated	CVE-2021-28153 MISC
gnutls -- gnutls	A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.	2021-03-12	not yet calculated	CVE-2021-20232 MISC MISC
gnutls -- gnutls	A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.	2021-03-12	not yet calculated	CVE-2021-20231 MISC MISC
go -- go	archive/zip in Go 1.16.x before 1.16.1 allows attackers to cause a denial of service (panic) upon attempted use of the Reader.Open API for a ZIP archive in which ../ occurs at the beginning of any filename.	2021-03-11	not yet calculated	CVE-2021-27919 MISC
go -- go	encoding/xml in Go before 1.15.9 and 1.16.x before 1.16.1 has an infinite loop if a custom TokenReader (for xml.NewTokenDecoder) returns EOF in the middle of an element. This can occur in the Decode, DecodeElement, or Skip method.	2021-03-11	not yet calculated	CVE-2021-27918 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In DeltaPerformer::Write of delta_performer.cc, there is a possible use of untrusted input due to improper input validation. This could lead to a local bypass of defense in depth protections with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160800689	2021-03-10	not yet calculated	CVE-2021-0377 MISC
google -- android	In sound_trigger_event_alloc of platform.h, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-167663878	2021-03-10	not yet calculated	CVE-2021-0464 MISC
google -- android	In the FingerTipS touch screen driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157156744	2021-03-10	not yet calculated	CVE-2021-0458 MISC MISC
google -- android	In qtaguid_untag of xt_qtaguid.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-176919394References: Upstream kernel	2021-03-10	not yet calculated	CVE-2021-0399 MISC
google -- android	In bindServiceLocked of ActiveServices.java, there is a possible foreground service launch due to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173516292	2021-03-10	not yet calculated	CVE-2021-0398 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In Builtins::Generate_ArgumentsAdaptorTrampoline of builtins-arm.cc and related files, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-160610106	2021-03-10	not yet calculated	CVE-2021-0396 MISC
google -- android	In fts_driver_test_write of fts_proc.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157154534	2021-03-10	not yet calculated	CVE-2021-0459 MISC MISC
google -- android	In nci_proc_rf_management_ntf of nci_hrcv.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-164440989	2021-03-10	not yet calculated	CVE-2021-0371 MISC
google -- android	In the FingerTipS touch screen driver, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157155375	2021-03-10	not yet calculated	CVE-2021-0457 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In checkUriPermission and related functions of MediaProvider.java, there is a possible way to access external files due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-115619667	2021-03-10	not yet calculated	CVE-2021-0376 MISC
google -- android	In GenerateFaceMask of face.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-172005755	2021-03-10	not yet calculated	CVE-2021-0465 MISC
google -- android	In convertToHidl of convert.cpp, there is a possible out of bounds read due to uninitialized data from ReturnFrameworkMessage. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-154867068	2021-03-10	not yet calculated	CVE-2021-0463 MISC
google -- android	In the NXP NFC firmware, there is a possible insecure firmware update due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168799695	2021-03-10	not yet calculated	CVE-2021-0462 MISC
google -- android	In iaxxx_core_sensor_change_state of iaxxx-module.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-175124074	2021-03-10	not yet calculated	CVE-2021-0461 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In the FingerTipS touch screen driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-156739245	2021-03-10	not yet calculated	CVE-2021-0460 MISC
google -- android	In the Citadel chip firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174769927	2021-03-10	not yet calculated	CVE-2021-0456 MISC
google -- android	In oggpack_look of bitwise.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169829774	2021-03-10	not yet calculated	CVE-2021-0368 MISC
google -- android	In sdp_copy_raw_data of sdp_discovery.cc, there is a possible system compromise due to a double free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174052148	2021-03-10	not yet calculated	CVE-2021-0397 MISC
google -- android	In CrossProfileAppsServiceImpl.java, there is the possibility of an application's INTERACT_ACROSS_PROFILES grant state not displaying properly in the setting UI due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-166561076	2021-03-10	not yet calculated	CVE-2021-0369 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In various methods of WifiNetworkSuggestionsManager.java, there is a possible modification of suggested networks due to a missing permission check. This could lead to local escalation of privilege by a background user on the same device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174749461	2021-03-10	not yet calculated	CVE-2021-0390 MISC
google -- android	In Write of NxpMfcReader.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169259605	2021-03-10	not yet calculated	CVE-2021-0370 MISC
hhvm -- hhvm	The unserialize() function supported a type code, "S", which was meant to be supported only for APC serialization. This type code allowed arbitrary memory addresses to be accessed as if they were static StringData objects. This issue affected HHVM prior to v4.32.3, between versions 4.33.0 and 4.56.0, 4.57.0, 4.58.0, 4.58.1, 4.59.0, 4.60.0, 4.61.0, 4.62.0.	2021-03-11	not yet calculated	CVE-2020-1899 MISC CONFIRM
hhvm -- hhvm	When unserializing an object with dynamic properties HHVM needs to pre-reserve the full size of the dynamic property array before inserting anything into it. Otherwise the array might resize, invalidating previously stored references. This pre-reservation was not occurring in HHVM prior to v4.32.3, between versions 4.33.0 and 4.56.0, 4.57.0, 4.58.0, 4.58.1, 4.59.0, 4.60.0, 4.61.0, 4.62.0.	2021-03-11	not yet calculated	CVE-2020-1900 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hhvm -- hhvm	An incorrect size calculation in ldap_escape may lead to an integer overflow when overly long input is passed in, resulting in an out-of-bounds write. This issue affects HHVM prior to 4.56.2, all versions between 4.57.0 and 4.78.0, 4.79.0, 4.80.0, 4.81.0, 4.82.0, 4.83.0.	2021-03-10	not yet calculated	CVE-2020-1916 MISC CONFIRM
hhvm -- hhvm	xbuf_format_converter, used as part of exif_read_data, was appending a terminating null character to the generated string, but was not using its standard append char function. As a result, if the buffer was full, it would result in an out-of-bounds write. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	2021-03-10	not yet calculated	CVE-2020-1917 MISC MISC
hhvm -- hhvm	In-memory file operations (ie: using fopen on a data URI) did not properly restrict negative seeking, allowing for the reading of memory prior to the in-memory buffer. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	2021-03-10	not yet calculated	CVE-2020-1918 MISC MISC
hhvm -- hhvm	Incorrect bounds calculations in substr_compare could lead to an out-of-bounds read when the second string argument passed in is longer than the first. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	2021-03-10	not yet calculated	CVE-2020-1919 MISC MISC
hhvm -- hhvm	Due to incorrect string size calculations inside the preg_quote function, a large input string passed to the function can trigger an integer overflow leading to a heap overflow. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	2021-03-10	not yet calculated	CVE-2021-24025 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hhvm -- hhvm	The fb_unserialize function did not impose a depth limit for nested deserialization. That meant a maliciously constructed string could cause deserialization to recurse, leading to stack exhaustion. This issue affected HHVM prior to v4.32.3, between versions 4.33.0 and 4.56.0, 4.57.0, 4.58.0, 4.58.1, 4.59.0, 4.60.0, 4.61.0, 4.62.0.	2021-03-11	not yet calculated	CVE-2020-1898 MISC CONFIRM
hhvm -- hhvm	In the crypt function, we attempt to null terminate a buffer using the size of the input salt without validating that the offset is within the buffer. This issue affects HHVM versions prior to 4.56.3, all versions between 4.57.0 and 4.80.1, all versions between 4.81.0 and 4.93.1, and versions 4.94.0, 4.95.0, 4.96.0, 4.97.0, 4.98.0.	2021-03-10	not yet calculated	CVE-2020-1921 MISC MISC
hyperledger -- besu	Hyperledger Besu is an open-source, MainNet compatible, Ethereum client written in Java. In Besu before version 1.5.1 there is a denial-of-service vulnerability involving the HTTP JSON-RPC API service. If username and password authentication is enabled for the HTTP JSON-RPC API service, then prior to making any requests to an API endpoint the requestor must use the login endpoint to obtain a JSON web token (JWT) using their credentials. A single user can readily overload the login endpoint with invalid requests (incorrect password). As the supplied password is checked for validity on the main vertx event loop and takes a relatively long time this can cause the processing of other valid requests to fail. A valid username is required for this vulnerability to be exposed. This has been fixed in version 1.5.1.	2021-03-09	not yet calculated	CVE-2021-21369 MISC MISC MISC CONFIRM
ibm -- datapower_gateway	IBM DataPower Gateway V10 and V2018 could allow a local attacker with administrative privileges to execute arbitrary code on the system using a server-side requesr forgery attack. IBM X-Force ID: 193247.	2021-03-08	not yet calculated	CVE-2020-5014 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- datapower_gateway	IBM DataPower Gateway 10.0.0.0 through 10.0.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 189965.	2021-03-12	not yet calculated	CVE-2020-4831 XF CONFIRM
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to read and write specific files due to weak file permissions. IBM X-Force ID: 192469.	2021-03-11	not yet calculated	CVE-2020-4976 XF CONFIRM
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the SSL handshake response. IBM X-Force ID: 193660.	2021-03-11	not yet calculated	CVE-2020-5024 XF CONFIRM
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 db2fm is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 193661.	2021-03-11	not yet calculated	CVE-2020-5025 XF CONFIRM
ibm -- spss_modeler_subscription	A vulnerability exists in IBM SPSS Modeler Subscription Installer that allows a user with create symbolic link permission to write arbitrary file in another protected path during product installation. IBM X-Force ID: 187727.	2021-03-10	not yet calculated	CVE-2020-4717 XF CONFIRM
ibm -- tivoli_netcool	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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.	2021-03-11	not yet calculated	CVE-2021-20336 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. When application security is disabled and JAX-RPC applications are present, an attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary xml files on the system. This does not occur if Application security is enabled. IBM X-Force ID: 193556.	2021-03-10	not yet calculated	CVE-2020-5016 XF CONFIRM
imagemagick -- imagemagick	A flaw was found in ImageMagick in coders/webp.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	2021-03-09	not yet calculated	CVE-2021-20245 MISC MISC
imagemagick -- magickcore	A flaw was found in ImageMagick in MagickCore/visual-effects.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	2021-03-09	not yet calculated	CVE-2021-20244 MISC MISC
imagemagick -- magickcore	A flaw was found in ImageMagick in MagickCore/resample.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	2021-03-09	not yet calculated	CVE-2021-20246 MISC
is-svg -- is-svg	The is-svg package 2.1.0 through 4.2.1 for Node.js uses a regular expression that is vulnerable to Regular Expression Denial of Service (ReDoS). If an attacker provides a malicious string, is-svg will get stuck processing the input for a very long time.	2021-03-12	not yet calculated	CVE-2021-28092 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jspdf -- jspdf	This affects the package jspdf before 2.3.1. ReDoS is possible via the addImage function.	2021-03-09	not yet calculated	CVE-2021-23353 MISC MISC MISC MISC MISC MISC MISC
kentico -- cms	The Blog module in Kentico CMS 5.5 R2 build 5.5.3996 allows SQL injection via the tagname parameter.	2021-03-05	not yet calculated	CVE-2021-27581 MISC MISC MISC
lenovo -- xclarity_administrator	An internal product security audit of LXCO, prior to version 1.2.2, discovered that credentials for Lenovo XClarity Administrator (LXCA), if added as a Resource Manager, are encoded then written to an internal LXCO log file each time a session is established with LXCA. Affected logs are captured in the First Failure Data Capture (FFDC) service log. The FFDC service log is only generated when requested by a privileged LXCO user and it is only accessible to the privileged LXCO user that requested the file.	2021-03-09	not yet calculated	CVE-2021-3417 MISC
leptonica -- leptonica	Leptonica before 1.80.0 allows a heap-based buffer over-read in pixReadFromTiffStream, related to tiffio.c.	2021-03-12	not yet calculated	CVE-2020-36280 MISC MISC MISC
leptonica -- leptonica	Leptonica before 1.80.0 allows a heap-based buffer over-read in findNextBorderPixel in ccbord.c.	2021-03-12	not yet calculated	CVE-2020-36278 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
leptonica -- leptonica	Leptonica before 1.80.0 allows a heap-based buffer over-read in pixFewColorsOctcubeQuantMixed in colorquant1.c.	2021-03-12	not yet calculated	CVE-2020-36281 MISC MISC MISC
leptonica -- leptonica	Leptonica before 1.80.0 allows a heap-based buffer over-read in rasteropGeneralLow, related to adaptmap_reg.c and adaptmap.c.	2021-03-12	not yet calculated	CVE-2020-36279 MISC MISC MISC
leptonica -- leptonica	Leptonica before 1.80.0 allows a denial of service (application crash) via an incorrect left shift in pixConvert2To8 in pixconv.c.	2021-03-11	not yet calculated	CVE-2020-36277 MISC MISC MISC
lib3mf -- lib3mf	A use-after-free vulnerability exists in the NMR::COpcPackageReader::releaseZIP() functionality of 3MF Consortium lib3mf 2.0.0. A specially crafted 3MF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-03-10	not yet calculated	CVE-2021-21772 MISC
libjpeg-turbo -- libjpeg-turbo	Libjpeg-turbo versions 2.0.91 and 2.0.90 is vulnerable to a denial of service vulnerability caused by a divide by zero when processing a crafted GIF image.	2021-03-10	not yet calculated	CVE-2021-20205 MISC
libtiff -- libtiff	An integer overflow flaw was found in libtiff that exists in the tif_getimage.c file. This flaw allows an attacker to inject and execute arbitrary code when a user opens a crafted TIFF file. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-03-09	not yet calculated	CVE-2020-35523 MISC MISC MISC DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libtiff -- libtiff	A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially crafted TIFF file can lead to arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-03-09	not yet calculated	CVE-2020-35524 MISC MISC MISC DEBIAN
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.	2021-03-07	not yet calculated	CVE-2021-27365 MISC MISC MISC MLIST MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.	2021-03-07	not yet calculated	CVE-2021-27363 MISC MISC MISC MLIST
linux -- linux_kernel	An out-of-bounds access flaw was found in the Linux kernel's implementation of the eBPF code verifier in the way a user running the eBPF script calls dev_map_init_map or sock_map_alloc. This flaw allows a local user to crash the system or possibly escalate their privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-03-09	not yet calculated	CVE-2021-20268 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	A flaw was found in the way memory resources were freed in the unix_stream_recvmsg function in the Linux kernel when a signal was pending. This flaw allows an unprivileged local user to crash the system by exhausting available memory. The highest threat from this vulnerability is to system availability.	2021-03-10	not yet calculated	CVE-2021-20265 MISC MISC
linux -- linux_kernel	A race condition was found in the Linux kernels implementation of the floppy disk drive controller driver software. The impact of this issue is lessened by the fact that the default permissions on the floppy device (/dev/fd0) are restricted to root. If the permissions on the device have changed the impact changes greatly. In the default configuration root (or equivalent) permissions are required to attack this flaw.	2021-03-11	not yet calculated	CVE-2021-20261 MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.	2021-03-07	not yet calculated	CVE-2021-27364 MISC MISC MLIST MISC
lucy -- security_awareness_software	LUCY Security Awareness Software through 4.7.x allows unauthenticated remote code execution because the Migration Tool (in the support section) allows upload of .php files within a system.tar.gz file. The .php file becomes accessible with a public/system/static URI.	2021-03-11	not yet calculated	CVE-2021-28132 MISC
lxco -- lxco	An internal product security audit of LXCO, prior to version 1.2.2, discovered that optional passwords, if specified, for the Syslog and SMTP forwarders are written to an internal LXCO log file in clear text. Affected logs are captured in the First Failure Data Capture (FFDC) service log. The FFDC service log is only generated when requested by a privileged LXCO user and it is only accessible to the privileged LXCO user that requested the file.	2021-03-09	not yet calculated	CVE-2020-8356 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
magicconnect -- client	Untrusted search path vulnerability in Installer of MagicConnect Client program distributed before 2021 March 1 allows an attacker to gain privileges and via a Trojan horse DLL in an unspecified directory and to execute arbitrary code with the privilege of the user invoking the installer when a terminal is connected remotely using Remote desktop.	2021-03-12	not yet calculated	CVE-2021-20674 MISC MISC
microsoft -- azure	Azure Sphere Unsigned Code Execution Vulnerability This CVE ID is unique from CVE-2021-27074.	2021-03-11	not yet calculated	CVE-2021-27080 MISC
microsoft -- azure	Azure Virtual Machine Information Disclosure Vulnerability	2021-03-11	not yet calculated	CVE-2021-27075 MISC
microsoft -- azure	Azure Sphere Unsigned Code Execution Vulnerability This CVE ID is unique from CVE-2021-27080.	2021-03-11	not yet calculated	CVE-2021-27074 MISC
microsoft -- directx	DirectX Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-24095 MISC
microsoft -- excel	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27053.	2021-03-11	not yet calculated	CVE-2021-27054 MISC
microsoft -- excel	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27054.	2021-03-11	not yet calculated	CVE-2021-27053 MISC
microsoft -- internet_explorer	Internet Explorer Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27085 MISC
microsoft -- internet_explorer	Internet Explorer Memory Corruption Vulnerability	2021-03-11	not yet calculated	CVE-2021-26411 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- office	Microsoft Office ClickToRun Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27058 MISC
microsoft -- office	Microsoft Office Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24108, CVE-2021-27059.	2021-03-11	not yet calculated	CVE-2021-27057 MISC
microsoft -- office	Microsoft Office Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24108, CVE-2021-27057.	2021-03-11	not yet calculated	CVE-2021-27059 MISC
microsoft -- office	Microsoft Office Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27057, CVE-2021-27059.	2021-03-11	not yet calculated	CVE-2021-24108 MISC
microsoft -- onetype_font	OpenType Font Parsing Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-26876 MISC
microsoft -- power_bi_report_server	Microsoft Power BI Information Disclosure Vulnerability	2021-03-11	not yet calculated	CVE-2021-26859 MISC
microsoft -- powerpoint	Microsoft PowerPoint Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27056 MISC
microsoft -- sharepoint	Microsoft SharePoint Server Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27076 MISC MISC
microsoft -- sharepoint	Microsoft SharePoint Server Information Disclosure Vulnerability	2021-03-11	not yet calculated	CVE-2021-27052 MISC
microsoft -- sharepoint	Microsoft SharePoint Spoofing Vulnerability	2021-03-11	not yet calculated	CVE-2021-24104 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- visio	Microsoft Visio Security Feature Bypass Vulnerability	2021-03-11	not yet calculated	CVE-2021-27055 MISC
microsoft -- visual_studio	Visual Studio Code Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27060 MISC
microsoft -- windows	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26894, CVE-2021-26895.	2021-03-11	not yet calculated	CVE-2021-26897 MISC
microsoft -- windows	Windows Print Spooler Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26878.	2021-03-11	not yet calculated	CVE-2021-1640 MISC
microsoft -- windows	Windows Update Stack Setup Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-1729 MISC
microsoft -- windows	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-26896.	2021-03-11	not yet calculated	CVE-2021-27063 MISC
microsoft -- windows	Windows 10 Update Assistant Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-27070 MISC
microsoft -- windows	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26877, CVE-2021-26893, CVE-2021-26894, CVE-2021-26897.	2021-03-11	not yet calculated	CVE-2021-26895 MISC
microsoft -- windows	Windows Event Tracing Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26872, CVE-2021-26901.	2021-03-11	not yet calculated	CVE-2021-26898 MISC
microsoft -- windows	Windows Graphics Component Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-26868 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	Windows ActiveX Installer Service Information Disclosure Vulnerability	2021-03-11	not yet calculated	CVE-2021-26869 MISC
microsoft -- windows	Windows Event Tracing Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26898, CVE-2021-26901.	2021-03-11	not yet calculated	CVE-2021-26872 MISC
microsoft -- windows	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-27063.	2021-03-11	not yet calculated	CVE-2021-26896 MISC
microsoft -- windows	Windows UPnP Device Host Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-26899 MISC
microsoft -- windows	Windows Event Tracing Information Disclosure Vulnerability	2021-03-11	not yet calculated	CVE-2021-24107 MISC
microsoft -- windows	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26863, CVE-2021-26875, CVE-2021-27077.	2021-03-11	not yet calculated	CVE-2021-26900 MISC
microsoft -- windows	Windows Event Tracing Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26872, CVE-2021-26898.	2021-03-11	not yet calculated	CVE-2021-26901 MISC
microsoft -- windows	Windows Projected File System Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-26870 MISC
microsoft -- windows	Windows Error Reporting Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-24090 MISC
microsoft -- windows	Windows WalletService Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26885.	2021-03-11	not yet calculated	CVE-2021-26871 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	Windows User Profile Service Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-26873 MISC
microsoft -- windows	Windows Overlay Filter Elevation of Privilege Vulnerability	2021-03-11	not yet calculated	CVE-2021-26874 MISC
microsoft -- windows	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26893, CVE-2021-26894, CVE-2021-26895, CVE-2021-26897.	2021-03-11	not yet calculated	CVE-2021-26877 MISC
microsoft -- windows	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26863, CVE-2021-26900, CVE-2021-27077.	2021-03-11	not yet calculated	CVE-2021-26875 MISC
microsoft -- windows	Windows Admin Center Security Feature Bypass Vulnerability	2021-03-11	not yet calculated	CVE-2021-27066 MISC
microsoft -- windows	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26863, CVE-2021-26875, CVE-2021-26900.	2021-03-11	not yet calculated	CVE-2021-27077 MISC
microsoft -- visual_studio	Visual Studio Code ESLint Extension Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27081 MISC
microsoft -- visual_studio	Quantum Development Kit for Visual Studio Code Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27082 MISC
microsoft -- visual_studio	Visual Studio Code Java Extension Pack Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27084 MISC
microsoft -- visual_studio	Remote Development Extension for Visual Studio Code Remote Code Execution Vulnerability	2021-03-11	not yet calculated	CVE-2021-27083 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
msgpack5 -- msgpack5	msgpack5 is a msgpack v5 implementation for node.js and the browser. In msgpack5 before versions 3.6.1, 4.5.1, and 5.2.1 there is a "Prototype Poisoning" vulnerability. When msgpack5 decodes a map containing a key "__proto__", it assigns the decoded value to __proto__. Object.prototype.__proto__ is an accessor property for the receiver's prototype. If the value corresponding to the key __proto__ decodes to an object or null, msgpack5 sets the decoded object's prototype to that value. An attacker who can submit crafted MessagePack data to a service can use this to produce values that appear to be of other types; may have unexpected prototype properties and methods (for example length, numeric properties, and push et al if __proto__'s value decodes to an Array); and/or may throw unexpected exceptions when used (for example if the __proto__ value decodes to a Map or Date). Other unexpected behavior might be produced for other types. There is no effect on the global prototype. This "prototype poisoning" is sort of a very limited inversion of a prototype pollution attack. Only the decoded value's prototype is affected, and it can only be set to msgpack5 values (though if the victim makes use of custom codecs, anything could be a msgpack5 value). We have not found a way to escalate this to true prototype pollution (absent other bugs in the consumer's code). This has been fixed in msgpack5 version 3.6.1, 4.5.1, and 5.2.1. See the referenced GitHub Security Advisory for an example and more details.	2021-03-12	not yet calculated	CVE-2021-21368 MISC MISC MISC MISC CONFIRM MISC
netgear -- jgs516pe/gs116ev2_devices	Multiple integer overflow parameters were found in the web administration panel on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices. Most of the integer parameters sent through the web server can be abused to cause a denial of service attack.	2021-03-10	not yet calculated	CVE-2020-35230 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- jgs516pe/gs116ev2_devices	The TFTP firmware update mechanism on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices does not properly implement firmware validations, allowing remote attackers to write arbitrary data to internal memory.	2021-03-10	not yet calculated	CVE-2020-35232 MISC
netgear -- jgs516pe/gs116ev2_devices	The CSRF protection mechanism implemented in the web administration panel on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices could be bypassed by omitting the CSRF token parameter in HTTP requests.	2021-03-10	not yet calculated	CVE-2020-35223 MISC
netgear -- jgs516pe/gs116ev2_devices	The NSDP protocol implementation on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was not properly validating the length of string parameters sent in write requests, potentially allowing denial of service attacks.	2021-03-10	not yet calculated	CVE-2020-35225 MISC
netgear -- jgs516pe/gs116ev2_devices	NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allow unauthenticated users to modify the switch DHCP configuration by sending the corresponding write request command.	2021-03-10	not yet calculated	CVE-2020-35226 MISC
netgear -- jgs516pe/gs116ev2_devices	The NSDP protocol implementation on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was affected by an authentication issue that allows an attacker to bypass access controls and obtain full control of the device.	2021-03-10	not yet calculated	CVE-2020-35231 MISC
netgear -- jgs516pe/gs116ev2_devices	The authentication token required to execute NSDP write requests on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices is not properly invalidated and can be reused until a new token is generated, which allows attackers (with access to network traffic) to effectively gain administrative privileges.	2021-03-10	not yet calculated	CVE-2020-35229 MISC
netgear -- jgs516pe/gs116ev2_devices	A buffer overflow vulnerability in the access control section on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices (in the administration web panel) allows an attacker to inject IP addresses into the whitelist via the checkedList parameter to the delete command.	2021-03-10	not yet calculated	CVE-2020-35227 MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- jgs516pe/gs116ev2_devices	A buffer overflow vulnerability in the NSDP protocol authentication method on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allows remote unauthenticated attackers to force a device reboot.	2021-03-10	not yet calculated	CVE-2020-35224 MISC
netgear -- jgs516pe/gs116ev2_devices	The NSDP protocol version implemented on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allows unauthenticated remote attackers to obtain all the switch configuration parameters by sending the corresponding read requests.	2021-03-10	not yet calculated	CVE-2020-35222 MISC
netgear -- jgs516pe/gs116ev2_devices	The hashing algorithm implemented for NSDP password authentication on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was found to be insecure, allowing attackers (with access to a network capture) to quickly generate multiple collisions to generate valid passwords, or infer some parts of the original.	2021-03-10	not yet calculated	CVE-2020-35221 MISC
netgear -- jgs516pe/gs116ev2_devices	A cross-site scripting (XSS) vulnerability in the administration web panel on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices allows remote attackers to inject arbitrary web script or HTML via the language parameter.	2021-03-10	not yet calculated	CVE-2020-35228 MISC
netgear -- jgs516pe/gs116ev2_devices	A TFTP server was found to be active by default on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices. It allows remote authenticated users to update the switch firmware.	2021-03-10	not yet calculated	CVE-2020-35220 MISC
netgear -- jgs516pe/gs116ev2_devices	The TFTP server fails to handle multiple connections on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices, and allows external attackers to force device reboots by sending concurrent connections, aka a denial of service attack.	2021-03-10	not yet calculated	CVE-2020-35233 MISC

TLP:WHITE

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netty -- netty	Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.60.Final there is a vulnerability that enables request smuggling. If a Content-Length header is present in the original HTTP/2 request, the field is not validated by `Http2MultiplexHandler` as it is propagated up. This is fine as long as the request is not proxied through as HTTP/1.1. If the request comes in as an HTTP/2 stream, gets converted into the HTTP/1.1 domain objects (`HttpRequest`, `HttpContent`, etc.) via `Http2StreamFrameToHttpObjectCodec `and then sent up to the child channel's pipeline and proxied through a remote peer as HTTP/1.1 this may result in request smuggling. In a proxy case, users may assume the content-length is validated somehow, which is not the case. If the request is forwarded to a backend channel that is a HTTP/1.1 connection, the Content-Length now has meaning and needs to be checked. An attacker can smuggle requests inside the body as it gets downgraded from HTTP/2 to HTTP/1.1. For an example attack refer to the linked GitHub Advisory. Users are only affected if all of this is true: `HTTP2MultiplexCodec` or `Http2FrameCodec` is used, `Http2StreamFrameToHttpObjectCodec` is used to convert to HTTP/1.1 objects, and these HTTP/1.1 objects are forwarded to another remote peer. This has been patched in 4.1.60.Final As a workaround, the user can do the validation by themselves by implementing a custom `ChannelInboundHandler` that is put in the `ChannelPipeline` behind `Http2StreamFrameToHttpObjectCodec`.	2021-03-09	not yet calculated	CVE-2021-21295 MISC MISC CONFIRM
nginx -- nginx	An integer buffer overflow in the Nginx webserver of ExpressVPN Router version 1 allows remote attackers to obtain sensitive information when the server running as reverse proxy via specially crafted request.	2021-03-10	not yet calculated	CVE-2020-29238 MISC MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
october -- october	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October before version 1.1.2, when running on poorly configured servers (i.e. the server routes any request, regardless of the HOST header to an October CMS instance) the potential exists for Host Header Poisoning attacks to succeed. This has been addressed in version 1.1.2 by adding a feature to allow a set of trusted hosts to be specified in the application. As a workaround one may set the configuration setting cms.linkPolicy to force.	2021-03-10	not yet calculated	CVE-2021-21265 MISC MISC CONFIRM
open5gs -- open5gs	A request-validation issue was discovered in Open5GS 2.1.3 through 2.2.0. The WebUI component allows an unauthenticated user to use a crafted HTTP API request to create, read, update, or delete entries in the subscriber database. For example, new administrative users can be added. The issue occurs because Express is not set up to require authentication.	2021-03-10	not yet calculated	CVE-2021-28122 MISC MISC MISC
pjsip -- pjsip	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In PJSIP version 2.10 and earlier, after an initial INVITE has been sent, when two 183 responses are received, with the first one causing negotiation failure, a crash will occur. This results in a denial of service.	2021-03-10	not yet calculated	CVE-2021-21375 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pjsip -- pjsip	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In version 2.10 and earlier, PJSIP transport can be reused if they have the same IP address + port + protocol. However, this is insufficient for secure transport since it lacks remote hostname authentication. Suppose we have created a TLS connection to `sip.foo.com`, which has an IP address `100.1.1.1`. If we want to create a TLS connection to another hostname, say `sip.bar.com`, which has the same IP address, then it will reuse that existing connection, even though `100.1.1.1` does not have certificate to authenticate as `sip.bar.com`. The vulnerability allows for an insecure interaction without user awareness. It affects users who need access to connections to different destinations that translate to the same address, and allows man-in-the-middle attack if attacker can route a connection to another destination such as in the case of DNS spoofing.	2021-03-10	not yet calculated	CVE-2020-15260 MISC MISC CONFIRM
powerlogic -- multiple_products	A CWE-119:Improper restriction of operations within the bounds of a memory buffer vulnerability exists in PowerLogic ION8650, ION8800, ION7650, ION7700/73xx, and ION83xx/84xx/85xx/8600 (see security notifcation for affected versions), which could cause the meter to reboot.	2021-03-11	not yet calculated	CVE-2021-22713 MISC
powerlogic -- multiple_products	A CWE-119:Improper restriction of operations within the bounds of a memory buffer vulnerability exists in PowerLogic ION7400, PM8000 and ION9000 (All versions prior to V3.0.0), which could cause the meter to reboot or allow for remote code execution.	2021-03-11	not yet calculated	CVE-2021-22714 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
printf -- printf	The package printf before 0.6.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the regex string /\%(?:\(([\w_.]+)\)|([1-9]\d*)\$)?([0 +\-\]*)(*|\d+)?(\.)?(*|\d+)?[hlL]?([\%bscdeEfFgGioOuxX])/g in lib/printf.js. The vulnerable regular expression has cubic worst-case time complexity.	2021-03-12	not yet calculated	CVE-2021-23354 CONFIRM CONFIRM CONFIRM
pupnp -- pupnp	A stack overflow in pupnp 1.16.1 can cause the denial of service through the Parser_parseDocument() function. ixmlNode_free() will release a child node recursively, which will consume stack space and lead to a crash.	2021-03-12	not yet calculated	CVE-2021-28302 MISC
qemu -- eepro100_i8255x_devices	A stack overflow via an infinite recursion vulnerability was found in the eepro100 i8255x device emulator of QEMU. This issue occurs while processing controller commands due to a DMA reentry issue. This flaw allows a guest user or process to consume CPU cycles or crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	2021-03-09	not yet calculated	CVE-2021-20255 MISC MISC MISC
qemu -- qemu	A flaw was found in the virtio-fs shared file system daemon (virtiofsd) of QEMU. The new 'xattrmap' option may cause the 'security.capability' xattr in the guest to not drop on file write, potentially leading to a modified, privileged executable in the guest. In rare circumstances, this flaw could be used by a malicious user to elevate their privileges within the guest.	2021-03-09	not yet calculated	CVE-2021-20263 MISC MISC
quadbase -- espressreports	An issue was discovered in Quadbase EspressReports ES 7 Update 9. An unauthenticated attacker can create a malicious HTML file that houses a POST request made to the DashboardBuilder within the target web application. This request will utilise the target admin session and perform the authenticated request (to change the Dashboard name) as if the victim had done so themselves, aka CSRF.	2021-03-11	not yet calculated	CVE-2020-24983 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
quadbase -- espressreports	An issue was discovered in Quadbase EspressReports ES 7 Update 9. It allows CSRF, whereby an attacker may be able to trick an authenticated admin level user into uploading malicious files to the web server.	2021-03-11	not yet calculated	CVE-2020-24984 MISC
rabbitmq -- rabbitmq	JMS Client for RabbitMQ 1.x before 1.15.2 and 2.x before 2.2.0 is vulnerable to unsafe deserialization that can result in code execution via crafted StreamMessage data.	2021-03-12	not yet calculated	CVE-2020-36282 MISC MISC MISC MISC
redhat -- keycloak	A flaw was found in Keycloak 12.0.0 where re-authentication does not occur while updating the password. This flaw allows an attacker to take over an account if they can obtain temporary, physical access to a user's browser. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-03-09	not yet calculated	CVE-2021-20262 MISC
redhat -- keycloak	A flaw was found in keycloak in versions prior to 13.0.0. The client registration endpoint allows fetching information about PUBLIC clients (like client secret) without authentication which could be an issue if the same PUBLIC client changed to CONFIDENTIAL later. The highest threat from this vulnerability is to data confidentiality.	2021-03-08	not yet calculated	CVE-2020-27838 MISC
rust -- rust	An issue was discovered in the fltk crate before 0.15.3 for Rust. There is an out-of bounds read because the pixmap constructor lacks pixmap input validation.	2021-03-12	not yet calculated	CVE-2021-28308 MISC
rust -- rust	An issue was discovered in the fltk crate before 0.15.3 for Rust. There is a NULL pointer dereference during attempted use of a multi label type if the image is nonexistent.	2021-03-12	not yet calculated	CVE-2021-28306 MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rust -- rust	An issue was discovered in the fltk crate before 0.15.3 for Rust. There is a NULL pointer dereference during attempted use of a non-raster image for a window icon.	2021-03-12	not yet calculated	CVE-2021-28307 MISC
rust -- rust	An issue was discovered in the diesel crate before 1.4.6 for Rust. There is a use-after-free in the SQLite backend because the semantics of sqlite3_column_name are not followed.	2021-03-12	not yet calculated	CVE-2021-28305 MISC
sap -- 3d_visual_enterprise_viewer	When a user opens manipulated Graphics Interchange Format (.GIF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	2021-03-09	not yet calculated	CVE-2021-21493 MISC MISC
sap -- enterprise_financial_services	SAP Enterprise Financial Services versions, 101, 102, 103, 104, 105, 600, 603, 604, 605, 606, 616, 617, 618, 800, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2021-03-09	not yet calculated	CVE-2021-21486 MISC MISC
sap -- hana_database	LDAP authentication in SAP HANA Database version 2.0 can be bypassed if the attached LDAP directory server is configured to enable unauthenticated bind.	2021-03-09	not yet calculated	CVE-2021-21484 MISC MISC
sap -- knowledge_management	Knowledge Management versions 7.01, 7.02, 7.30, 7.31, 7.40, 7.50 allows a remote attacker with basic privileges to deserialize user-controlled data without verification, leading to insecure deserialization which triggers the attacker's code, therefore impacting Availability.	2021-03-09	not yet calculated	CVE-2021-21488 MISC MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- mii	SAP MII allows users to create dashboards and save them as JSP through the SSCE (Self Service Composition Environment). An attacker can intercept a request to the server, inject malicious JSP code in the request and forward to server. When this dashboard is opened by Users having at least SAP_XMII_Developer role, malicious content in the dashboard gets executed, leading to remote code execution in the server, which allows privilege escalation. The malicious JSP code can contain certain OS commands, through which an attacker can read sensitive files in the server, modify files or even delete contents in the server thus compromising the confidentiality, integrity and availability of the server hosting the SAP MII application.	2021-03-09	not yet calculated	CVE-2021-21480 MISC MISC
sap -- netweaver	The MigrationService, which is part of SAP NetWeaver versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform an authorization check. This might allow an unauthorized attacker to access configuration objects, including such that grant administrative privileges. This could result in complete compromise of system confidentiality, integrity, and availability.	2021-03-09	not yet calculated	CVE-2021-21481 MISC MISC
sap -- netweaver_application_server	SAP Netweaver Application Server Java (Applications based on WebDynpro Java) versions 7.00, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allow an attacker to redirect users to a malicious site due to Reverse Tabnabbing vulnerabilities.	2021-03-10	not yet calculated	CVE-2021-21491 MISC MISC
sap -- payment_engine	SAP Payment Engine version 500, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2021-03-09	not yet calculated	CVE-2021-21487 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
schneider_electric -- igss	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to missing validation of input data.	2021-03-11	not yet calculated	CVE-2021-22711 MISC MISC
schneider_electric -- igss	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in loss of data or remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	2021-03-11	not yet calculated	CVE-2021-22709 MISC MISC
schneider_electric -- igss	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could cause remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	2021-03-11	not yet calculated	CVE-2021-22710 MISC MISC
schneider_electric -- igss	A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to an unchecked pointer address.	2021-03-11	not yet calculated	CVE-2021-22712 MISC MISC
simatic -- mv400	In SIMATIC MV400 family versions prior to v7.0.6, the ISN generator is initialized with a constant value and has constant increments. An attacker could predict and hijack TCP sessions.	2021-03-10	not yet calculated	CVE-2020-27632 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sonicwall -- sma100	A post-authenticated vulnerability in SonicWall SMA100 allows an attacker to export the configuration file to the specified email address. This vulnerability impacts SMA100 version 10.2.0.5 and earlier.	2021-03-13	not yet calculated	CVE-2021-20018 CONFIRM
sonicwall -- sma100	A post-authenticated command injection vulnerability in SonicWall SMA100 allows an authenticated attacker to execute OS commands as a 'nobody' user. This vulnerability impacts SMA100 version 10.2.0.5 and earlier.	2021-03-13	not yet calculated	CVE-2021-20017 CONFIRM
spdk -- spdk	An issue was discovered in Storage Performance Development Kit (SPDK) before 20.01.01. If a PDU is sent to the iSCSI target with a zero length (but data is expected), the iSCSI target can crash with a NULL pointer dereference.	2021-03-13	not yet calculated	CVE-2021-28361 MISC
ssri -- ssri	ssri 5.2.2-8.0.0, fixed in 8.0.1, processes SRIs using a regular expression which is vulnerable to a denial of service. Malicious SRIs could take an extremely long time to process, leading to denial of service. This issue only affects consumers using the strict option.	2021-03-12	not yet calculated	CVE-2021-27290 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
swagger-codegen -- swagger-codegen	swagger-codegen is an open-source project which contains a template-driven engine to generate documentation, API clients and server stubs in different languages by parsing your OpenAPI / Swagger definition. In swagger-codegen before version 2.4.19, on Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory. This vulnerability is local privilege escalation because the contents of the `outputFolder` can be appended to by an attacker. As such, code written to this directory, when executed can be attacker controlled. For more details refer to the referenced GitHub Security Advisory. This vulnerability is fixed in version 2.4.19. Note this is a distinct vulnerability from CVE-2021-21364.	2021-03-11	not yet calculated	CVE-2021-21363 MISC CONFIRM
swagger-codegen -- swagger-codegen	swagger-codegen is an open-source project which contains a template-driven engine to generate documentation, API clients and server stubs in different languages by parsing your OpenAPI / Swagger definition. In swagger-codegen before version 2.4.19, on Unix-Like systems, the system temporary directory is shared between all local users. When files/directories are created, the default `umask` settings for the process are respected. As a result, by default, most processes/apis will create files/directories with the permissions `-rw-r--r--` and `drwxr-xr-x` respectively, unless an API that explicitly sets safe file permissions is used. Because this vulnerability impacts generated code, the generated code will remain vulnerable until fixed manually! This vulnerability is fixed in version 2.4.19. Note this is a distinct vulnerability from CVE-2021-21363.	2021-03-11	not yet calculated	CVE-2021-21364 MISC CONFIRM

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
switchboard -- bluetooth_plug	Switchboard Bluetooth Plug for elementary OS from version 2.3.0 and before version version 2.3.5 has an incorrect authorization vulnerability. When the Bluetooth plug is running (in discoverable mode), Bluetooth service requests and pairing requests are automatically accepted, allowing physically proximate attackers to pair with a device running an affected version of switchboard-plug-bluetooth without the active consent of the user. By default, elementary OS doesn't expose any services via Bluetooth that allow information to be extracted by paired Bluetooth devices. However, if such services (i.e. contact list sharing software) have been installed, it's possible that attackers have been able to extract data from such services without authorization. If no such services have been installed, attackers are only able to pair with a device running an affected version without authorization and then play audio out of the device or possibly present a HID device (keyboard, mouse, etc...) to control the device. As such, users should check the list of trusted/paired devices and remove any that are not 100% confirmed to be genuine. This is fixed in version 2.3.5. To reduce the likelihood of this vulnerability on an unpatched version, only open the Bluetooth plug for short intervals when absolutely necessary and preferably not in crowded public areas. To mitigate the risk entirely with unpatched versions, do not open the Bluetooth plug within switchboard at all, and use a different method for pairing devices if necessary (e.g. `bluetoothctl` CLI).	2021-03-12	not yet calculated	CVE-2021-21367 MISC MISC CONFIRM
synology -- diskstation_manager	Out-of-bounds Read vulnerability in iscsi_snapshot_comm_core in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via crafted web requests.	2021-03-12	not yet calculated	CVE-2021-27647 CONFIRM

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synology -- diskstation_manager	Use After Free vulnerability in iscsi_snapshot_comm_core in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via crafted web requests.	2021-03-12	not yet calculated	CVE-2021-27646 CONFIRM
synology -- diskstation_manager	Race Condition within a Thread vulnerability in iscsi_snapshot_comm_core in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via crafted web requests.	2021-03-12	not yet calculated	CVE-2021-26569 CONFIRM
telerik -- telerik	** DISPUTED ** An issue was discovered in Progress Telerik UI for ASP.NET AJAX 2021.1.224. It allows unauthorized access to MicrosoftAjax.js through the Telerik.Web.UI.WebResource.axd file. This may allow the attacker to gain unauthorized access to the server and execute code. To exploit, one must use the parameter _TSM_HiddenField_ and inject a command at the end of the URI. NOTE: the vendor states that this is not a vulnerability. The request's output does not indicate that a "true" command was executed on the server, and the request's output does not leak any private source code or data from the server.	2021-03-11	not yet calculated	CVE-2021-28141 MISC MISC
tenable -- jira_cloud	Tenable for Jira Cloud is an open source project designed to pull Tenable.io vulnerability data, then generate Jira Tasks and sub-tasks based on the vulnerabilities' current state. It published in pypi as "tenable-jira-cloud". In tenable-jira-cloud before version 1.1.21, it is possible to run arbitrary commands through the yaml.load() method. This could allow an attacker with local access to the host to run arbitrary code by running the application with a specially crafted YAML configuration file. This is fixed in version 1.1.21 by using yaml.safe_load() instead of yaml.load().	2021-03-10	not yet calculated	CVE-2021-21371 MISC CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tibco -- multiple_products	The Spotfire client component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Desktop, and TIBCO Spotfire Server contains a vulnerability that theoretically allows a low privileged attacker with network access to execute a stored Cross Site Scripting (XSS) attack on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 10.3.3 and below, versions 10.10.0, 10.10.1, and 10.10.2, versions 10.7.0, 10.8.0, 10.9.0, 11.0.0, and 11.1.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.1.0 and below, TIBCO Spotfire Desktop: versions 10.3.3 and below, versions 10.10.0, 10.10.1, and 10.10.2, versions 10.7.0, 10.8.0, 10.9.0, 11.0.0, and 11.1.0, and TIBCO Spotfire Server: versions 10.3.11 and below, versions 10.10.0, 10.10.1, 10.10.2, and 10.10.3, versions 10.7.0, 10.8.0, 10.8.1, 10.9.0, 11.0.0, and 11.1.0.	2021-03-09	not yet calculated	CVE-2021-23273 CONFIRM CONFIRM
tiny -- tiny_rss	The auth_internal plugin in Tiny Tiny RSS (aka tt-rss) before 2021-03-12 allows an attacker to log in via the OTP code without a valid password. NOTE: this issue only affected the git master branch for a short time. However, all end users are explicitly directed to use the git master branch in production. Semantic version numbers such as 21.03 appear to exist, but are automatically generated from the year and month. They are not releases.	2021-03-13	not yet calculated	CVE-2021-28373 MISC MISC
twinkle_tray -- twinkle_tray	Twinkle Tray (aka twinkle-tray) through 1.13.3 allows remote command execution. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which invokes the dangerous openExternal API.	2021-03-09	not yet calculated	CVE-2021-28119 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vxworks -- vxworks	** UNSUPPORTED WHEN ASSIGNED ** A DNS client stack-based buffer overflow in ipdnsc_decode_name() affects Wind River VxWorks 6.5 through 7. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-03-11	not yet calculated	CVE-2016-20009 MISC
web_based_quiz_system -- web_based_quiz_system	Web Based Quiz System 1.0 is affected by cross-site scripting (XSS) in register.php through the name parameter.	2021-03-10	not yet calculated	CVE-2021-28007 MISC
weseek -- growi	Improper access control vulnerability in GROWI versions v4.2.2 and earlier allows a remote unauthenticated attacker to read the user's personal information and/or server's internal information via unspecified vectors.	2021-03-10	not yet calculated	CVE-2021-20670 MISC MISC
weseek -- growi	Invalid file validation on the upload feature in GROWI versions v4.2.2 allows a remote attacker with administrative privilege to overwrite the files on the server, which may lead to arbitrary code execution.	2021-03-10	not yet calculated	CVE-2021-20671 MISC MISC
weseek -- growi	Stored cross-site scripting vulnerability due to inadequate CSP (Content Security Policy) configuration in GROWI versions v4.2.2 and earlier allows remote authenticated attackers to inject an arbitrary script via a specially crafted content.	2021-03-10	not yet calculated	CVE-2021-20667 MISC MISC
weseek -- growi	Path traversal vulnerability in GROWI versions v4.2.2 and earlier allows an attacker with administrator rights to read an arbitrary path via a specially crafted URL.	2021-03-10	not yet calculated	CVE-2021-20668 MISC MISC
weseek -- growi	Path traversal vulnerability in GROWI versions v4.2.2 and earlier allows an attacker with administrator rights to read and/or delete an arbitrary path via a specially crafted URL.	2021-03-10	not yet calculated	CVE-2021-20669 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
weseek -- growi	Stored cross-site scripting vulnerability in Admin Page of GROWI (v4.2 Series) versions from v4.2.0 to v4.2.7 allows remote authenticated attackers to inject an arbitrary script via unspecified vectors.	2021-03-10	not yet calculated	CVE-2021-20673 MISC MISC
weseek -- growi	Reflected cross-site scripting vulnerability due to insufficient verification of URL query parameters in GROWI (v4.2 Series) versions from v4.2.0 to v4.2.7 allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-03-10	not yet calculated	CVE-2021-20672 MISC MISC
western_digital -- my_cloud_os_5_devices	Western Digital My Cloud OS 5 devices before 5.10.122 mishandle Symbolic Link Following on SMB and AFP shares. This can lead to code execution and information disclosure (by reading local files).	2021-03-10	not yet calculated	CVE-2021-3310 MISC MISC
wordpress -- wordpress	The food-and-drink-menu plugin through 2.2.0 for WordPress allows remote attackers to execute arbitrary code because of an unserialize operation on the fdm_cart cookie in load_cart_from_cookie in includes/class-cart-manager.php.	2021-03-11	not yet calculated	CVE-2020-29045 MISC MISC
xmldom -- xmldom	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) DOMParser and XMLSerializer module. xmldom versions 0.4.0 and older do not correctly preserve system identifiers, FPIs or namespaces when repeatedly parsing and serializing maliciously crafted documents. This may lead to unexpected syntactic changes during XML processing in some downstream applications. This is fixed in version 0.5.0. As a workaround downstream applications can validate the input and reject the maliciously crafted documents.	2021-03-12	not yet calculated	CVE-2021-21366 MISC MISC CONFIRM MISC

TLP:WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki_platform -- xwiki_platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions of XWiki Platform, the `{{wikimacrocontent}}` executes the content with the rights of the wiki macro author instead of the caller of that wiki macro. This makes possible to inject scripts through it and they will be executed with the rights of the wiki macro (very often a user which has Programming rights). Fortunately, no such macro exists by default in XWiki Standard but one could have been created or installed with an extension. This vulnerability has been patched in versions XWiki 12.6.3, 11.10.11 and 12.8-rc-1. There is no easy workaround other than disabling the affected macros. Inserting content in a safe way or knowing what is the user who called the wiki macro is not easy.	2021-03-12	not yet calculated	CVE-2021-21379 CONFIRM MISC
zoho_manageengine -- servicedesk_plus	Zoho ManageEngine ServiceDesk Plus before 11134 allows an Authentication Bypass (only during SAML login).	2021-03-13	not yet calculated	CVE-2020-35682 MISC
zte -- multiple_products	Some ZTE products have an input verification vulnerability in the diagnostic function interface. Due to insufficient verification of some parameters input by users, an attacker with high privileges can cause process exception by repeatedly inputting illegal parameters. This affects:<ZXONE 9700 , ZXONE 8700, ZXONE 19700><V1.40.021.021CP049, V1.0P02B219_@NCPM-RELEASE_2.40R1-20200914.set>	2021-03-12	not yet calculated	CVE-2021-21726 MISC

Back to top

This product is provided subject to this Notification and this Privacy & Use policy.

TLP:WHITE