

# WinSecure Full Scan Report

Generated: Fri May 9 19:35:17 2025

## Network Scan Results

| IP Address                             | Category      |
|--|---------------|
| 255.255.255.255                        | non-malicious |
| 192.168.1.1                            | non-malicious |
| 192.168.56.255                         | non-malicious |
| 192.168.1.255                          | non-malicious |
| 192.168.1.5                            | non-malicious |
| 172.26.95.255                          | non-malicious |
| 2404:6800:4003:c1c::bc                 | non-malicious |
| 2606:4700:90d2:7cbc:c2c5:408:5ff2:75c4 | non-malicious |
| 2600:1417:6a::b819:6da3                | non-malicious |
| 2603:1040:a06:6::2                     | non-malicious |
| 20.189.173.24                          | non-malicious |
| 2603:1040:603:c::d5                    | non-malicious |
| 20.167.82.225                          | non-malicious |
| 2603:1040:a06:6::1                     | non-malicious |
| 104.46.162.226                         | non-malicious |
| 13.107.137.11                          | non-malicious |
| 13.89.179.13                           | non-malicious |
| 140.82.114.25                          | non-malicious |
| 2620:1ec:bdf::68                       | non-malicious |
| 2606:4700:90d2:7cbc:c2ca:4d5:5ff2:75c4 | non-malicious |
| 52.104.12.25                           | non-malicious |

## System Vulnerability Results

| Software | Version | CVE_ID | Severity | Score | Description |
|----------|---------|--------|----------|-------|-------------|
|----------|---------|--------|----------|-------|-------------|

|       |                 |                      |        |      |  |
|-------|-----------------|----------------------|--------|------|--|
| Brave | 136.1.78.9<br>7 | CVE-2016-9473        | MEDIUM | 4.7  | Brave Browser iOS before 1.2.18 and Brave Browser Android 1.9.56 and earlier suffer from Full Address Bar Spoofing, allowing attackers to trick a victim by displaying a malicious page for legitimate domain names.   |
| Brave | 136.1.78.9<br>7 | CVE-2017-8458        | None   | None | Brave 0.12.4 has a URI Obfuscation issue in which a string such as <code>https://safe.example.com@unsafe.example.com/</code> is displayed without a clear UI indication that it is not a resource on the <code>safe.example.com</code> web site.   |
| Brave | 136.1.78.9<br>7 | CVE-2017-8459        | MEDIUM | 5.3  | Brave 0.12.4 has a Status Bar Obfuscation issue in which a redirection target is shown in a possibly unexpected way. NOTE: third parties dispute this issue because it is a behavior that might have legitimate applications in (for example) the display of web-search results                                |
| Brave | 136.1.78.9<br>7 | CVE-2017-100046<br>1 | None   | None | Brave Software's Brave Browser, version 0.19.73 (and earlier) is vulnerable to an incorrect access control issue in the "JS fingerprinting blocking" component, resulting in a malicious website being able to access the fingerprinting-associated browser functionality (that the browser intends to block). |
| Brave | 136.1.78.9<br>7 | CVE-2016-10718       | None   | None | Brave Browser before 0.13.0 allows a tab to close itself even if the tab was not opened by a script, resulting in denial of service.   |
| Brave | 136.1.78.9<br>7 | CVE-2017-18256       | None   | None | Brave Browser before 0.13.0 allows remote attackers to cause a denial of service (resource consumption) via a long <code>alert()</code> argument in JavaScript code, because window dialogs are mishandled.  |
| Brave | 136.1.78.9<br>7 | CVE-2018-10798       | None   | None | A hang issue was discovered in Brave before 0.14.0 (on, for example, Linux). The vulnerability is caused by mishandling of JavaScript code that triggers the reload of a page continuously with an interval of 1 second.   |
| Brave | 136.1.78.9<br>7 | CVE-2018-10799       | None   | None | A hang issue was discovered in Brave before 0.14.0 (on, for example, Linux). This vulnerability is caused by the mishandling of a long URL formed by <code>window.location+='?\u202a\uFEFF\u202b'</code> ; concatenation in a SCRIPT element.  |

|       |                 |                      |                      |            |  |
|-------|-----------------|----------------------|----------------------|------------|--|
| Brave | 136.1.78.9<br>7 | CVE-2018-100081<br>5 | None                 | None       | Brave Software Inc. Brave version version 0.22.810 to 0.24.0 contains a Other/Unknown vulnerability in function ContentSettingsObserver::AllowScript() in content_settings_observer.cc that can result in Websites can run inline JavaScript even if script is blocked, making attackers easier to track users. This attack appear to be exploitable via the victim must visit a specially crafted website. This vulnerability appears to have been fixed in 0.25.2.   |
| Brave | 136.1.78.9<br>7 | CVE-2020-8276        | MEDIUM               | 5.5        | The implementation of Brave Desktop's privacy-preserving analytics system (P3A) between 1.1 and 1.18.35 logged the timestamp of when the user last opened an incognito window, including Tor windows. The intended behavior was to log the timestamp for incognito windows excluding Tor windows. Note that if a user has P3A enabled, the timestamp is not sent to Brave's server, but rather a value from:Used in last 24hUsed in last week but not 24hUsed in last 28 days but not weekEver used but not in last 28 daysNever usedThe privacy risk is low because a local attacker with disk access cannot tell if the timestamp corresponds to a Tor window or a non-Tor incognito window. |
| Brave | 136.1.78.9<br>7 | CVE-2021-21323       | ['MEDIUM', 'MEDIUM'] | [4.3, 5.3] | Brave is an open source web browser with a focus on privacy and security. In Brave versions 1.17.73-1.20.103, the CNAME adblocking feature added in Brave 1.17.73 accidentally initiated DNS requests that bypassed the Brave Tor proxy. Users with adblocking enabled would leak DNS requests from Tor windows to their DNS provider. (DNS requests that were not initiated by CNAME adblocking would go through Tor as expected.) This is fixed in Brave version 1.20.108  |
| Brave | 136.1.78.9<br>7 | CVE-2021-22916       | MEDIUM               | 5.9        | In Brave Desktop between versions 1.17 and 1.26.60, when adblocking is enabled and a proxy browser extension is installed, the CNAME adblocking feature issues DNS requests that used the system DNS settings instead of the extension's proxy settings, resulting in possible information disclosure.   |
| Brave | 136.1.78.9<br>7 | CVE-2021-22917       | MEDIUM               | 6.5        | Brave Browser Desktop between versions 1.17 and 1.20 is vulnerable to information disclosure by way of DNS requests in Tor windows not flowing through Tor if adblocking was enabled.  |
| Brave | 136.1.78.9<br>7 | CVE-2021-22929       | MEDIUM               | 6.1        | An information disclosure exists in Brave Browser Desktop prior to version 1.28.62, where logged warning messages that included timestamps of connections to V2 onion domains in tor.log.  |

|       |                 |                |                        |            |   |
|-------|-----------------|----------------|------------------------|------------|---|
| Brave | 136.1.78.9<br>7 | CVE-2021-45884 | HIGH                   | 7.5        | In Brave Desktop 1.17 through 1.33 before 1.33.106, when CNAME-based adblocking and a proxying extension with a SOCKS fallback are enabled, additional DNS requests are issued outside of the proxying extension using the system's DNS settings, resulting in information disclosure. NOTE: this issue exists because of an incomplete fix for CVE-2021-21323 and CVE-2021-22916.  |
| Brave | 136.1.78.9<br>7 | CVE-2022-30334 | MEDIUM                 | 5.3        | Brave before 1.34, when a Private Window with Tor Connectivity is used, leaks .onion URLs in Referer and Origin headers. NOTE: although this was fixed by Brave, the Brave documentation still advises "Note that Private Windows with Tor Connectivity in Brave are just regular private windows that use Tor as a proxy. Brave does NOT implement most of the privacy protections from Tor Browser."                    |
| Brave | 136.1.78.9<br>7 | CVE-2022-47932 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | Brave Browser before 1.43.34 allowed a remote attacker to cause a denial of service via a crafted HTML file that mentions an ipfs:// or ipns:// URL. This vulnerability is caused by an incomplete fix for CVE-2022-47933.  |
| Brave | 136.1.78.9<br>7 | CVE-2022-47933 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | Brave Browser before 1.42.51 allowed a remote attacker to cause a denial of service via a crafted HTML file that references the IPFS scheme. This vulnerability is caused by an uncaught exception in the function ipfs::OnBeforeURLRequest_IPFSRedirectWork() in ipfs_redirect_network_delegate_helper.c.  |
| Brave | 136.1.78.9<br>7 | CVE-2022-47934 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | Brave Browser before 1.43.88 allowed a remote attacker to cause a denial of service in private and guest windows via a crafted HTML file that mentions an ipfs:// or ipns:// URL. This is caused by an incomplete fix for CVE-2022-47932 and CVE-2022-47934.  |
| Brave | 136.1.78.9<br>7 | CVE-2021-4281  | ['MEDIUM', 'CRITICAL'] | [4.6, 9.8] | A vulnerability was found in Brave UX for-the-badge and classified as critical. Affected by this issue is some unknown functionality of the file .github/workflows/combine-prs.yml. The manipulation leads to os command injection. The name of the patch is 55b5a234c0fab935df5fb08365bc8fe9c37cf46b. It is recommended to apply a patch to fix this issue. VDB-216842 is the identifier assigned to this vulnerability. |

|       |                 |                |                         |               |   |
|-------|-----------------|----------------|-------------------------|---------------|---|
| Brave | 136.1.78.9<br>7 | CVE-2023-22798 | ['MEDIUM',<br>'MEDIUM'] | [6.1,<br>6.1] | Prior to commit 51867e0d15a6d7f80d5b714fd0e9976b9c160bb0, <a href="https://github.com/brave/adblock-lists">https://github.com/brave/adblock-lists</a> removed redirect interceptors on some websites like Facebook in which the redirect interceptor may have been there for security purposes. This could potentially cause open redirects on these websites. Brave's redirect interceptor removal feature is known as "debouncing" and is intended to remove unnecessary redirects that track users across the web. |
| Brave | 136.1.78.9<br>7 | CVE-2023-28360 | ['MEDIUM',<br>'MEDIUM'] | [4.3,<br>4.3] | An omission of security-relevant information vulnerability exists in Brave desktop prior to version 1.48.171 when a user was saving a file there was no download safety check dialog presented to the user.   |
| Brave | 136.1.78.9<br>7 | CVE-2023-28364 | MEDIUM                  | 6.1           | An Open Redirect vulnerability exists prior to version 1.52.117, where the built-in QR scanner in Brave Browser Android navigated to scanned URLs automatically without showing the URL first. Now the user must manually navigate to the URL.  |
| Brave | 136.1.78.9<br>7 | CVE-2023-52263 | MEDIUM                  | 6.1           | Brave Browser before 1.59.40 does not properly restrict the schema for WebUI factory and redirect. This is related to browser/brave_content_browser_client.cc and browser/ui/webui/brave_web_ui_controller_factory.cc.  |
| Brave | 136.1.78.9<br>7 | CVE-2023-51534 | ['MEDIUM',<br>'MEDIUM'] | [5.9,<br>4.8] | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brave Brave â Create Popup, Optins, Lead Generation, Survey, Sticky Elements & Interactive Content allows Stored XSS.This issue affects Brave â Create Popup, Optins, Lead Generation, Survey, Sticky Elements & Interactive Content: from n/a through 0.6.2.   |
| Brave | 136.1.78.9<br>7 | CVE-2024-30453 | MEDIUM                  | 5.4           | Server-Side Request Forgery (SSRF) vulnerability in Brave Brave Popup Builder.This issue affects Brave Popup Builder: from n/a through 0.6.5.   |
| Brave | 136.1.78.9<br>7 | CVE-2024-35655 | ['MEDIUM',<br>'MEDIUM'] | [5.9,<br>4.8] | Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brave Brave Popup Builder allows Stored XSS.This issue affects Brave Popup Builder: from n/a through 0.6.9.  |
| Brave | 136.1.78.9<br>7 | CVE-2024-43337 | ['MEDIUM',<br>'MEDIUM'] | [4.3,<br>4.3] | Cross-Site Request Forgery (CSRF) vulnerability in Brave Brave Popup Builder.This issue affects Brave Popup Builder: from n/a through 0.7.0.  |
| Brave | 136.1.78.9<br>7 | CVE-2024-37406 | HIGH                    | 7.5           | In Brave Android prior to v1.67.116, domains in the Brave Shields popup are elided from the right instead of the left, which may lead to domain confusion.  |

|                            |                 |                |                  |            |  |
|----------------------------|-----------------|----------------|------------------|------------|--|
| Brave                      | 136.1.78.9<br>7 | CVE-2024-56609 | None             | None       | In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: use ieee80211_purge_tx_queue() to purge TX skb When removing kernel modules by: rmmod rtw88_8723cs rtw88_8703b rtw88_8723x rtw88_sdio rtw88_core Driver uses skb_queue_purge() to purge TX skb, but not report tx status causing "Have pending ack frames!" warning. Use ieee80211_purge_tx_queue() to correct this. Since ieee80211_purge_tx_queue() doesn't take locks, to prevent racing between TX work and purge TX queue, flush and destroy TX work in advance. wlan0: deauthenticating from aa:f5:fd:60:4c:a8 by local choice (Reason: 3=DEAUTH_LEAVING) -----[ cut here ] ----- Have pending ack frames! WARNING: CPU: 3 PID: 9232 at net/mac80211/main.c:1691 ieee80211_free_ack_frame+0x5c/0x90 [mac80211] CPU: 3 PID: 9232 Comm: rmmod Tainted: G C 6.10.1-200.fc40.aarch64 #1 Hardware name: pine64 Pine64 PinePhone Braveheart (1.1)/Pine64 PinePhone Bravehear... |
| Brave                      | 136.1.78.9<br>7 | CVE-2025-23086 | MEDIUM           | 6.1        | On most desktop platforms, Brave Browser versions 1.70.x-1.73.x included a feature to show a site's origin on the OS-provided file selector dialog when a site prompts the user to upload or download a file. However the origin was not correctly inferred in some cases. When combined with an open redirector vulnerability on a trusted site, this could allow a malicious site to initiate a download whose origin in the file select dialog appears as the trusted site which initiated the redirect.  |
| Brave                      | 136.1.78.9<br>7 | CVE-2025-0862  | MEDIUM           | 4.9        | The SuperSaaS â online appointment scheduling plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the âafterâ parameter in all versions up to, and including, 2.1.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is limited to Chromium-based browsers (e.g. Chrome, Edge, Brave).   |
| Dell Power Manager Service | 3.7.0           | CVE-2023-25543 | ['HIGH', 'HIGH'] | [7.8, 7.8] | Dell Power Manager, versions prior to 3.14, contain an Improper Authorization vulnerability in DPM service. A low privileged malicious user could potentially exploit this vulnerability in order to elevate privileges on the system.   |

|                    |           |                |                  |            |  |
|--------------------|-----------|----------------|------------------|------------|--|
| Dell SupportAssist | 3.8.0.108 | CVE-2018-1214  | None             | None       | Dell EMC SupportAssist Enterprise version 1.1 creates a local Windows user account named "OMEAdapterUser" with a default password as part of the installation process. This unnecessary user account also remains even after an upgrade from v1.1 to v1.2. Access to the management console can be achieved by someone with knowledge of the default password. If SupportAssist Enterprise is installed on a server running OpenManage Essentials (OME), the OmeAdapterUser user account is added as a member of the OmeAdministrators group for the OME. An unauthorized person with knowledge of the default password and access to the OME web console could potentially use this account to gain access to the affected installation of OME with OmeAdministrators privileges. This is fixed in version 1.2.1. |
| Dell SupportAssist | 3.8.0.108 | CVE-2019-3718  | HIGH             | 8.8        | Dell SupportAssist Client versions prior to 3.2.0.90 contain an improper origin validation vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability to attempt CSRF attacks on users of the impacted systems.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2019-3719  | HIGH             | 8.0        | Dell SupportAssist Client versions prior to 3.2.0.90 contain a remote code execution vulnerability. An unauthenticated attacker, sharing the network access layer with the vulnerable system, can compromise the vulnerable system by tricking a victim user into downloading and executing arbitrary executables via SupportAssist client from attacker hosted sites.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2019-3735  | HIGH             | 7.8        | Dell SupportAssist for Business PCs version 2.0 and Dell SupportAssist for Home PCs version 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, and 3.2.1 contain an Improper Privilege Management Vulnerability. A malicious local user can exploit this vulnerability by inheriting a system thread using a leaked thread handle to gain system privileges on the affected machine.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2021-21518 | ['HIGH', 'HIGH'] | [7.8, 7.8] | 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.   |

|                    |           |                |                  |            |   |
|--------------------|-----------|----------------|------------------|------------|---|
| Dell SupportAssist | 3.8.0.108 | CVE-2020-5316  | ['HIGH', 'HIGH'] | [7.8, 7.8] | Dell SupportAssist for Business PCs versions 2.0, 2.0.1, 2.0.2, 2.1, 2.1.1, 2.1.2, 2.1.3 and Dell SupportAssist for Home PCs version 2.0, 2.0.1, 2.0.2, 2.1, 2.1.1, 2.1.2, 2.1.3, 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, 3.2.1, 3.2.2, 3.3, 3.3.1, 3.3.2, 3.3.3, 3.4 contain an uncontrolled search path vulnerability. A locally authenticated low privileged user could exploit this vulnerability to cause the loading of arbitrary DLLs by the SupportAssist binaries, resulting in the privileged execution of arbitrary code.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2021-36286 | ['HIGH', 'HIGH'] | [7.1, 7.1] | Dell SupportAssist Client Consumer versions 3.9.13.0 and any versions prior to 3.9.13.0 contain an arbitrary file deletion vulnerability that can be exploited by using the Windows feature of NTFS called Symbolic links. Symbolic links can be created by any(non-privileged) user under some object directories, but by themselves are not sufficient to successfully escalate privileges. However, combining them with a different object, such as the NTFS junction point allows for the exploitation. Support assist clean files functionality do not distinguish junction points from the physical folder and proceeds to clean the target of the junction that allows nonprivileged users to create junction points and delete arbitrary files on the system which can be accessed only by the admin. |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-29092 | ['HIGH', 'HIGH'] | [7.8, 7.8] | Dell SupportAssist Client Consumer versions (3.11.0 and versions prior) and Dell SupportAssist Client Commercial versions (3.2.0 and versions prior) contain a privilege escalation vulnerability. A non-admin user can exploit the vulnerability and gain admin access to the system.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-29093 | ['HIGH', 'HIGH'] | [7.1, 7.1] | Dell SupportAssist Client Consumer versions (3.10.4 and versions prior) and Dell SupportAssist Client Commercial versions (3.1.1 and versions prior) contain an arbitrary file deletion vulnerability. Authenticated non-admin user could exploit the issue and delete arbitrary files on the system.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-29094 | ['HIGH', 'HIGH'] | [7.1, 7.1] | Dell SupportAssist Client Consumer versions (3.10.4 and versions prior) and Dell SupportAssist Client Commercial versions (3.1.1 and versions prior) contain an arbitrary file deletion/overwrite vulnerability. Authenticated non-admin user could exploit the issue and delete or overwrite arbitrary files on the system.  |

|                    |           |                |                      |            |   |
|--------------------|-----------|----------------|----------------------|------------|---|
| Dell SupportAssist | 3.8.0.108 | CVE-2022-29095 | ['HIGH', 'CRITICAL'] | [8.3, 9.6] | Dell SupportAssist Client Consumer versions (3.10.4 and prior) and Dell SupportAssist Client Commercial versions (3.1.1 and prior) contain a cross-site scripting vulnerability. A remote unauthenticated malicious user could potentially exploit this vulnerability under specific conditions leading to execution of malicious code on a vulnerable system.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-34366 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Dell SupportAssist for Home PCs (version 3.11.2 and prior) contain Overly Permissive Cross-domain Whitelist vulnerability. An authenticated non-admin user could potentially exploit the issue and obtain sensitive information.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-34384 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Dell SupportAssist Client Consumer (version 3.11.1 and prior), SupportAssist Client Commercial (version 3.2 and prior), Dell Command   Update, Dell Update, and Alienware Update versions before 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user may potentially exploit this vulnerability, leading to privilege escalation. |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-34386 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Dell SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain cryptographic weakness vulnerability. An authenticated non-admin user could potentially exploit the issue and obtain sensitive information.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-34387 | ['MEDIUM', 'HIGH']   | [6.4, 7.8] | Dell SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain a privilege escalation vulnerability. A local authenticated malicious user could potentially exploit this vulnerability to elevate privileges and gain total control of the system.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-34388 | ['HIGH', 'HIGH']     | [7.1, 7.1] | Dell SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain information disclosure vulnerability. A local malicious user with low privileges could exploit this vulnerability to view and modify sensitive information in the database of the affected application.   |
| Dell SupportAssist | 3.8.0.108 | CVE-2022-34389 | ['LOW', 'MEDIUM']    | [3.7, 5.3] | Dell SupportAssist contains a rate limit bypass issues in screenmeet API third party component. An unauthenticated attacker could potentially exploit this vulnerability and impersonate a legitimate dell customer to a dell support technician.   |

|                    |           |                |                      |            |  |
|--------------------|-----------|----------------|----------------------|------------|--|
| Dell SupportAssist | 3.8.0.108 | CVE-2023-48670 | ['HIGH', 'HIGH']     | [7.3, 7.8] | Dell SupportAssist for Home PCs version 3.14.1 and prior versions contain a privilege escalation vulnerability in the installer. A local low privileged authenticated attacker may potentially exploit this vulnerability, leading to the execution of arbitrary executable on the operating system with elevated privileges.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2023-25535 | ['HIGH', 'MEDIUM']   | [7.2, 6.5] | Dell SupportAssist for Home PCs Installer Executable file version prior to 3.13.2.19 used for initial installation has a high vulnerability that can result in local privilege escalation (LPE). This vulnerability only affects first-time installations done prior to 8th March 2023   |
| Dell SupportAssist | 3.8.0.108 | CVE-2023-39249 | ['MEDIUM', 'MEDIUM'] | [6.3, 5.3] | Dell SupportAssist for Business PCs version 3.4.0 contains a local Authentication Bypass vulnerability that allows locally authenticated non-admin users to gain temporary privilege within the SupportAssist User Interface on their respective PC. The Run as Admin temporary privilege feature enables IT/System Administrators to perform driver scans and Dell-recommended driver installations without requiring them to log out of the local non-admin user session. However, the granted privilege is limited solely to the SupportAssist User Interface and automatically expires after 15 minutes. |
| Dell SupportAssist | 3.8.0.108 | CVE-2023-44283 | ['HIGH', 'HIGH']     | [7.8, 7.8] | In Dell SupportAssist for Home PCs (between v3.0 and v3.14.1) and SupportAssist for Business PCs (between v3.0 and v3.4.1), a security concern has been identified, impacting locally authenticated users on their respective PCs. This issue may potentially enable privilege escalation and the execution of arbitrary code, in the Windows system context, and confined to that specific local PC.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2024-38305 | ['HIGH', 'HIGH']     | [7.3, 7.3] | Dell SupportAssist for Home PCs Installer exe version 4.0.3 contains a privilege escalation vulnerability in the installer. A local low-privileged authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary executables on the operating system with elevated privileges.  |
| Dell SupportAssist | 3.8.0.108 | CVE-2024-52535 | ['HIGH', 'HIGH']     | [7.1, 8.8] | Dell SupportAssist for Home PCs versions 4.6.1 and prior and Dell SupportAssist for Business PCs versions 4.5.0 and prior, contain a symbolic link (symlink) attack vulnerability in the software remediation component. A low-privileged authenticated user could potentially exploit this vulnerability, gaining privileges escalation, leading to arbitrary deletion of files and folders from the system.  |

|                                |             |                |                  |            |   |
|--------------------------------|-------------|----------------|------------------|------------|---|
| Dell SupportAssist             | 3.8.0.108   | CVE-2025-22480 | ['HIGH', 'HIGH'] | [7.0, 7.8] | Dell SupportAssist OS Recovery versions prior to 5.5.13.1 contain a symbolic link attack vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary file deletion and Elevation of Privileges.   |
| Dell SupportAssist Remediation | 5.4.0.14842 | CVE-2024-52535 | ['HIGH', 'HIGH'] | [7.1, 8.8] | Dell SupportAssist for Home PCs versions 4.6.1 and prior and Dell SupportAssist for Business PCs versions 4.5.0 and prior, contain a symbolic link (symlink) attack vulnerability in the software remediation component. A low-privileged authenticated user could potentially exploit this vulnerability, gaining privileges escalation, leading to arbitrary deletion of files and folders from the system. |
| Docker Desktop                 | 4.33.1      | CVE-2019-15752 | ['HIGH', 'HIGH'] | [7.8, 7.8] | Docker Desktop Community Edition before 2.1.0.1 allows local users to gain privileges by placing a Trojan horse docker-credential-wincred.exe file in %PROGRAMDATA%\DockerDesktop\version-bin\ as a low-privilege user, and then waiting for an admin or service user to authenticate with Docker, restart Docker, or run 'docker login' to force the command.  |
| Docker Desktop                 | 4.33.1      | CVE-2020-10665 | MEDIUM           | 6.7        | Docker Desktop allows local privilege escalation to NT AUTHORITY\SYSTEM because it mishandles the collection of diagnostics with Administrator privileges, leading to arbitrary DACL permissions overwrites and arbitrary file writes. This affects Docker Desktop Enterprise before 2.1.0.9, Docker Desktop for Windows Stable before 2.2.0.4, and Docker Desktop for Windows Edge before 2.2.2.0.           |
| Docker Desktop                 | 4.33.1      | CVE-2020-11492 | HIGH             | 7.8        | An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.   |
| Docker Desktop                 | 4.33.1      | CVE-2020-15360 | HIGH             | 7.8        | com.docker.vmmnetd in Docker Desktop 2.3.0.3 allows privilege escalation because of a lack of client verification.  |
| Docker Desktop                 | 4.33.1      | CVE-2021-3162  | HIGH             | 7.8        | Docker Desktop Community before 2.5.0.0 on macOS mishandles certificate checking, leading to local privilege escalation.  |

|                |        |                |                    |            |   |
|----------------|--------|----------------|--------------------|------------|---|
| Docker Desktop | 4.33.1 | CVE-2021-37841 | HIGH               | 7.8        | Docker Desktop before 3.6.0 suffers from incorrect access control. If a low-privileged account is able to access the server running the Windows containers, it can lead to a full container compromise in both process isolation and Hyper-V isolation modes. This security issue leads an attacker with low privilege to read, write and possibly even execute code inside the containers. |
| Docker Desktop | 4.33.1 | CVE-2021-45449 | MEDIUM             | 5.5        | Docker Desktop version 4.3.0 and 4.3.1 has a bug that may log sensitive information (access token or password) on the user's machine during login. This only affects users if they are on Docker Desktop 4.3.0, 4.3.1 and the user has logged in while on 4.3.0, 4.3.1. Gaining access to this data would require having access to the user's local files.                                  |
| Docker Desktop | 4.33.1 | CVE-2022-23774 | MEDIUM             | 5.3        | Docker Desktop before 4.4.4 on Windows allows attackers to move arbitrary files.  |
| Docker Desktop | 4.33.1 | CVE-2022-25365 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Docker Desktop before 4.5.1 on Windows allows attackers to move arbitrary files. NOTE: this issue exists because of an incomplete fix for CVE-2022-23774.   |
| Docker Desktop | 4.33.1 | CVE-2022-26659 | HIGH               | 7.1        | Docker Desktop installer on Windows in versions before 4.6.0 allows an attacker to overwrite any administrator writable files by creating a symlink in place of where the installer writes its log file. Starting from version 4.6.0, the Docker Desktop installer, when run elevated, will write its log files to a location not writable by non-administrator users.                      |
| Docker Desktop | 4.33.1 | CVE-2021-44719 | HIGH               | 8.4        | Docker Desktop 4.3.0 has Incorrect Access Control.  |
| Docker Desktop | 4.33.1 | CVE-2023-0628  | ['MEDIUM', 'HIGH'] | [6.1, 7.8] | Docker Desktop before 4.17.0 allows an attacker to execute an arbitrary command inside a Dev Environments container during initialization by tricking a user to open a crafted malicious docker-desktop:// URL.   |

|                |        |                |                      |            |   |
|----------------|--------|----------------|----------------------|------------|---|
| Docker Desktop | 4.33.1 | CVE-2023-0629  | ['HIGH', 'HIGH']     | [7.1, 7.1] | Docker Desktop before 4.17.0 allows an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions by setting the Docker host to docker.raw.sock, or npipe:///pipe/docker_engine_linux on Windows, via the -H (--host) CLI flag or the DOCKER_HOST environment variable and launch containers without the additional hardening features provided by ECI. This would not affect already running containers, nor containers launched through the usual approach (without Docker's raw socket). The affected functionality is available for Docker Business customers only and assumes an environment where users are not granted local root or Administrator privileges. This issue has been fixed in Docker Desktop 4.17.0. Affected Docker Desktop versions: from 4.13.0 before 4.17.0. |
| Docker Desktop | 4.33.1 | CVE-2023-1802  | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | In Docker Desktop 4.17.x the Artifactory Integration falls back to sending registry credentials over plain HTTP if the HTTPS health check has failed. A targeted network sniffing attack can lead to a disclosure of sensitive information. Only users who have Access Experimental Features enabled and have logged in to a private registry are affected.   |
| Docker Desktop | 4.33.1 | CVE-2022-31647 | ['HIGH', 'HIGH']     | [7.1, 7.1] | Docker Desktop before 4.6.0 on Windows allows attackers to delete any file through the hyperv/destroy dockerBackendV2 API via a symlink in the DataFolder parameter, a different vulnerability than CVE-2022-26659.   |
| Docker Desktop | 4.33.1 | CVE-2022-34292 | ['HIGH', 'HIGH']     | [7.1, 7.1] | Docker Desktop for Windows before 4.6.0 allows attackers to overwrite any file through a symlink attack on the hyperv/create dockerBackendV2 API by controlling the DataFolder parameter for DockerDesktop.vhdx, a similar issue to CVE-2022-31647.   |
| Docker Desktop | 4.33.1 | CVE-2022-37326 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Docker Desktop for Windows before 4.6.0 allows attackers to delete (or create) any file through the dockerBackendV2 windowscontainers/start API by controlling the pidfile field inside the DaemonJSON field in the WindowsContainerStartRequest class. This can indirectly lead to privilege escalation.   |
| Docker Desktop | 4.33.1 | CVE-2022-38730 | ['MEDIUM', 'MEDIUM'] | [6.3, 6.3] | Docker Desktop for Windows before 4.6 allows attackers to overwrite any file through the windowscontainers/start dockerBackendV2 API by controlling the data-root field inside the DaemonJSON field in the WindowsContainerStartRequest class. This allows exploiting a symlink vulnerability in ..\dataRoot\network\files\local-kv.db because of a TOCTOU race condition.  |

|                |        |               |                      |            |  |
|----------------|--------|---------------|----------------------|------------|--|
| Docker Desktop | 4.33.1 | CVE-2023-0625 | ['HIGH', 'CRITICAL'] | [8.0, 9.8] | Docker Desktop before 4.12.0 is vulnerable to RCE via a crafted extension description or changelog. This issue affects Docker Desktop: before 4.12.0.  |
| Docker Desktop | 4.33.1 | CVE-2023-0626 | ['HIGH', 'CRITICAL'] | [8.0, 9.8] | Docker Desktop before 4.12.0 is vulnerable to RCE via query parameters in message-box route. This issue affects Docker Desktop: before 4.12.0.   |
| Docker Desktop | 4.33.1 | CVE-2023-0627 | ['MEDIUM', 'HIGH']   | [6.7, 7.8] | Docker Desktop 4.11.x allows --no-windows-containers flag bypass via IPC response spoofing which may lead to Local Privilege Escalation (LPE). This issue affects Docker Desktop: 4.11.X.  |
| Docker Desktop | 4.33.1 | CVE-2023-0633 | ['HIGH', 'HIGH']     | [7.2, 7.8] | In Docker Desktop on Windows before 4.12.0 an argument injection to installer may result in local privilege escalation (LPE). This issue affects Docker Desktop: before 4.12.0.  |
| Docker Desktop | 4.33.1 | CVE-2023-5165 | ['HIGH', 'HIGH']     | [7.1, 8.8] | Docker Desktop before 4.23.0 allows an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions via the debug shell which remains accessible for a short time window after launching Docker Desktop. The affected functionality is available for Docker Business customers only and assumes an environment where users are not granted local root or Administrator privileges. This issue has been fixed in Docker Desktop 4.23.0. Affected Docker Desktop versions: from 4.13.0 before 4.23.0. |
| Docker Desktop | 4.33.1 | CVE-2023-5166 | ['HIGH', 'MEDIUM']   | [8.0, 6.5] | Docker Desktop before 4.23.0 allows Access Token theft via a crafted extension icon URL. This issue affects Docker Desktop: before 4.23.0.   |

|                |        |                |                      |            |   |
|----------------|--------|----------------|----------------------|------------|---|
| Docker Desktop | 4.33.1 | CVE-2024-29018 | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | <p>Moby is an open source container framework that is a key component of Docker Engine, Docker Desktop, and other distributions of container tooling or runtimes. Moby's networking implementation allows for many networks, each with their own IP address range and gateway, to be defined. This feature is frequently referred to as custom networks, as each network can have a different driver, set of parameters and thus behaviors. When creating a network, the <code>--internal</code> flag is used to designate a network as <code>_internal_</code>. The <code>internal</code> attribute in a <code>docker-compose.yml</code> file may also be used to mark a network <code>_internal_</code>, and other API clients may specify the <code>internal</code> parameter as well. When containers with networking are created, they are assigned unique network interfaces and IP addresses. The host serves as a router for non-internal networks, with a gateway IP that provides SNAT/DNAT to/from container IPs. Containers on an internal network may communicate between each other, but are pre...</p> |
| Docker Desktop | 4.33.1 | CVE-2024-32473 | MEDIUM               | 4.7        | <p>Moby is an open source container framework that is a key component of Docker Engine, Docker Desktop, and other distributions of container tooling or runtimes. In 26.0.0, IPv6 is not disabled on network interfaces, including those belonging to networks where <code>--ipv6=false</code>. An container with an <code>ipvlan</code> or <code>macvlan</code> interface will normally be configured to share an external network link with the host machine. Because of this direct access, (1) Containers may be able to communicate with other hosts on the local network over link-local IPv6 addresses, (2) if router advertisements are being broadcast over the local network, containers may get SLAAC-assigned addresses, and (3) the interface will be a member of IPv6 multicast groups. This means interfaces in IPv4-only networks present an unexpectedly and unnecessarily increased attack surface. The issue is patched in 26.0.2. To completely disable IPv6 in a container, use <code>--sysctl=net.ipv6.conf.all.disable_ipv6=1</code> in the <code>docker create</code> ...</p>                 |
| Docker Desktop | 4.33.1 | CVE-2024-5652  | ['MEDIUM', 'MEDIUM'] | [6.1, 5.5] | <p>In Docker Desktop on Windows before v4.31.0Â allows a user in the <code>docker-users</code>Â group to cause a Windows Denial-of-Service through the <code>exec-path</code>Â Docker daemon config option in Windows containers mode.</p>  |

|                |        |                |          |      |  |
|----------------|--------|----------------|----------|------|--|
| Docker Desktop | 4.33.1 | CVE-2024-6222  | HIGH     | 7.0  | In Docker Desktop before v4.29.0, an attacker who has gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 <a href="https://docs.docker.com/desktop/release-notes/#4290">https://docs.docker.com/desktop/release-notes/#4290</a> fixes the issue on MacOS, Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker Desktop v4.31.0 <a href="https://docs.docker.com/desktop/release-notes/#4310">https://docs.docker.com/desktop/release-notes/#4310</a> additionally changes the default configuration to enable this setting by default.   |
| Docker Desktop | 4.33.1 | CVE-2024-8695  | CRITICAL | 9.8  | A remote code execution (RCE) vulnerability via crafted extension description/changelog could be abused by a malicious extension in Docker Desktop before 4.34.2.  |
| Docker Desktop | 4.33.1 | CVE-2024-8696  | CRITICAL | 9.8  | A remote code execution (RCE) vulnerability via crafted extension publisher-url/additional-urls could be abused by a malicious extension in Docker Desktop before 4.34.2.  |
| Docker Desktop | 4.33.1 | CVE-2024-9348  | None     | None | Docker Desktop before v4.34.3 allows RCE via unsanitized GitHub source link in Build view.   |
| Docker Desktop | 4.33.1 | CVE-2024-53182 | HIGH     | 7.8  | In the Linux kernel, the following vulnerability has been resolved: Revert "block, bfq: merge bfq_release_process_ref() into bfq_put_cooperator()" This reverts commit bc3b1e9e7c50e1de0f573eea3871db61dd4787de. The bic is associated with sync_bfq, and bfq_release_process_ref cannot be put into bfq_put_cooperator. kasan report: [ 400.347277]<br>===== [ 400.347287]<br>BUG: KASAN: slab-use-after-free in bic_set_bfq+0x200/0x230 [ 400.347420] Read of size 8 at addr ffff88881cab7d60 by task dockerd/5800 [ 400.347430] [ 400.347436] CPU: 24 UID: 0 PID: 5800 Comm: dockerd Kdump: loaded Tainted: G E 6.12.0 #32 [ 400.347450] Tainted: [E]=UNSIGNED_MODULE [ 400.347454] Hardware name: VMware, Inc. VMware20,1/440BX Desktop Reference Platform, BIOS VMW201.00V.20192059.B64.2207280713 07/28/2022 [ 400.347460] Call Trace: [ 400.347464] <TASK> [ 400.347468] dump_stack_lvl+0x5d/0x80 [ 400.347490] print_report+0x174/0x505 [ 400.347... |

|                |        |               |      |      |   |
|----------------|--------|---------------|------|------|---|
| Docker Desktop | 4.33.1 | CVE-2025-1696 | None | None | A vulnerability exists in Docker Desktop prior to version 4.39.0 that could lead to the unintentional disclosure of sensitive information via application logs. In affected versions, proxy configuration dataâpotentially including sensitive detailsâwas written to log files in clear text whenever an HTTP GET request was made through a proxy. An attacker with read access to these logs could obtain the proxy information and leverage it for further attacks or unauthorized access. Starting with version 4.39.0, Docker Desktop no longer logs the proxy string, thereby mitigating this risk.  |
| Docker Desktop | 4.33.1 | CVE-2025-3224 | None | None | A vulnerability in the update process of Docker Desktop for Windows versions prior to 4.41.0Â could allow a local, low-privileged attacker to escalate privileges to SYSTEM. During an update, Docker Desktop attempts to delete files and subdirectories under the path C:\ProgramData\Docker\config with high privileges. However, this directory often does not exist by default, and C:\ProgramData\ allows normal users to create new directories. By creating a malicious Docker\config folder structure at this location, an attacker can force the privileged update process to delete or manipulate arbitrary system files, leading to Elevation of Privilege. |
| Docker Desktop | 4.33.1 | CVE-2025-3911 | None | None | Recording of environment variables, configured for running containers, in Docker Desktop application logs could lead toÂ unintentional disclosure of sensitive information such as api keys, passwords, etc. A malicious actor with read access to these logs could obtain sensitive credentials information and further use it to gain unauthorized access to other systems. Starting with version 4.41.0, Docker Desktop no longer logs environment variables set by the user.  |
| Docker Desktop | 4.33.1 | CVE-2025-4095 | None | None | Registry Access Management (RAM) is a security feature allowing administrators to restrict access for their developers to only allowed registries. When a MacOS configuration profile is used to enforce organization sign-in, the RAM policies are not being applied, which would allow Docker Desktop users to pull down unapproved, and potentially malicious images from any registry.  |
| Git            | 2.45.2 | CVE-2006-0477 | None | None | Buffer overflow in git-checkout-index in GIT before 1.1.5 allows remote attackers to execute arbitrary code via an index file with a long symbolic link.  |

|     |        |               |      |      |   |
|-----|--------|---------------|------|------|---|
| Git | 2.45.2 | CVE-2008-3546 | None | None | Stack-based buffer overflow in the (1) diff_addremove and (2) diff_change functions in GIT before 1.5.6.4 might allow local users to execute arbitrary code via a PATH whose length is larger than the system's PATH_MAX when running GIT utilities such as git-diff or git-grep.   |
| Git | 2.45.2 | CVE-2008-5517 | None | None | The web interface in git (gitweb) 1.5.x before 1.5.6 allows remote attackers to execute arbitrary commands via shell metacharacters related to (1) git_snapshot and (2) git_object.   |
| Git | 2.45.2 | CVE-2008-5516 | None | None | The web interface in git (gitweb) 1.5.x before 1.5.5 allows remote attackers to execute arbitrary commands via shell metacharacters related to git_search.  |
| Git | 2.45.2 | CVE-2008-5916 | None | None | gitweb/gitweb.perl in gitweb in Git 1.6.x before 1.6.0.6, 1.5.6.x before 1.5.6.6, 1.5.5.x before 1.5.5.6, 1.5.4.x before 1.5.4.7, and other versions after 1.4.3 allows local repository owners to execute arbitrary commands by modifying the diff.external configuration variable and executing a crafted gitweb query. |
| Git | 2.45.2 | CVE-2009-2108 | None | None | git-daemon in git 1.4.4.5 through 1.6.3 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a request containing extra unrecognized arguments.   |
| Git | 2.45.2 | CVE-2010-0394 | None | None | PyGIT.py in the Trac Git plugin (trac-git) before 0.0.20080710-3+lenny1 and before 0.0.20090320-1 on Debian GNU/Linux, when enabled in Trac, allows remote attackers to execute arbitrary commands via shell metacharacters in a crafted HTTP query that is used to generate a certain git command.                       |
| Git | 2.45.2 | CVE-2010-2542 | None | None | Stack-based buffer overflow in the is_git_directory function in setup.c in Git before 1.7.2.1 allows local users to gain privileges via a long gitdir: field in a .git file in a working copy.  |
| Git | 2.45.2 | CVE-2010-3906 | None | None | Cross-site scripting (XSS) vulnerability in Gitweb 1.7.3.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) f and (2) fp parameters.  |
| Git | 2.45.2 | CVE-2011-1572 | None | None | Directory traversal vulnerability in the Admin Defined Commands (ADC) feature in gitolite before 1.5.9.1 allows remote attackers to execute arbitrary commands via .. (dot dot) sequences in admin-defined commands.  |

|     |        |               |      |      |   |
|-----|--------|---------------|------|------|---|
| Git | 2.45.2 | CVE-2012-0814 | None | None | The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory. |
| Git | 2.45.2 | CVE-2012-0054 | None | None | libs/updater.py in GoLismero 0.6.3, and other versions before Git revision 2b3bb43d6867, as used in backtrack and possibly other products, allows local users to overwrite arbitrary files via a symlink attack on GoLismero-controlled files, as demonstrated using Admin/changes.dat.   |
| Git | 2.45.2 | CVE-2012-2055 | HIGH | 7.5  | GitHub Enterprise before 20120304 does not properly restrict the use of a hash to provide values for a model's attributes, which allows remote attackers to set the public_key[user_id] value via a modified URL for the public-key update form, related to a "mass assignment" vulnerability.  |
| Git | 2.45.2 | CVE-2012-4506 | None | None | Directory traversal vulnerability in gitolite 3.x before 3.1, when wild card repositories and a pattern matching "../" are enabled, allows remote authenticated users to create arbitrary repositories and possibly perform other actions via a .. (dot dot) in a repository name.  |
| Git | 2.45.2 | CVE-2012-5814 | None | None | Weberknecht, as used in GitHub Gaug.es and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.   |
| Git | 2.45.2 | CVE-2013-0308 | None | None | The imap-send command in GIT before 1.8.1.4 does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.  |

|     |        |               |      |      |  |
|-----|--------|---------------|------|------|--|
| Git | 2.45.2 | CVE-2013-3670 | None | None | The rle_unpack function in vmdav.c in libavcodec in FFmpeg git 20130328 through 20130501 does not properly use the bytestream2 API, which allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) via crafted RLE data. NOTE: the vendor has listed this as an issue fixed in 1.2.1, but the issue is actually in new code that was not shipped with the 1.2.1 release or any earlier release. |
| Git | 2.45.2 | CVE-2013-7316 | None | None | Cross-site scripting (XSS) vulnerability in GitLab 6.0 and other versions before 6.5.0 allows remote attackers to inject arbitrary web script or HTML via a crafted HTML file, as demonstrated by README.html.   |
| Git | 2.45.2 | CVE-2013-4580 | None | None | GitLab before 5.4.2, Community Edition before 6.2.4, and Enterprise Edition before 6.2.1, when using a MySQL backend, allows remote attackers to impersonate arbitrary users and bypass authentication via unspecified API calls.  |
| Git | 2.45.2 | CVE-2013-4581 | None | None | GitLab 5.0 before 5.4.2, Community Edition before 6.2.4, Enterprise Edition before 6.2.1 and gitlab-shell before 1.7.8 allows remote attackers to execute arbitrary code via a crafted change using SSH.   |
| Git | 2.45.2 | CVE-2013-4490 | None | None | The SSH key upload feature (lib/gitlab_keys.rb) in gitlab-shell before 1.7.3, as used in GitLab 5.0 before 5.4.1 and 6.x before 6.2.3, allows remote authenticated users to execute arbitrary commands via shell metacharacters in the public key.   |
| Git | 2.45.2 | CVE-2013-4546 | None | None | The repository import feature in gitlab-shell before 1.7.4, as used in GitLab, allows remote authenticated users to execute arbitrary commands via the import URL.   |
| Git | 2.45.2 | CVE-2014-3456 | None | None | Cross-site scripting (XSS) vulnerability in GitLab Enterprise Edition (EE) 6.6.0 before 6.6.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.  |
| Git | 2.45.2 | CVE-2013-4489 | None | None | The Grit gem for Ruby, as used in GitLab 5.2 before 5.4.1 and 6.x before 6.2.3, allows remote authenticated users to execute arbitrary commands, as demonstrated by the search box for the GitLab code search feature.   |
| Git | 2.45.2 | CVE-2013-7392 | None | None | Gitlist allows remote attackers to execute arbitrary commands via shell metacharacters in a file name to Source/.  |

|     |        |               |      |      |   |
|-----|--------|---------------|------|------|---|
| Git | 2.45.2 | CVE-2014-4511 | None | None | Gitlist before 0.5.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the file name in the URI of a request for a (1) blame, (2) file, or (3) stats page, as demonstrated by requests to blame/master/, master/, and stats/master/.  |
| Git | 2.45.2 | CVE-2014-5023 | None | None | Repository.php in Gitter, as used in Gitlist, allows remote attackers with commit privileges to execute arbitrary commands via shell metacharacters in a branch name, as demonstrated by a "git checkout -b" command.   |
| Git | 2.45.2 | CVE-2014-5836 | None | None | The GittiGidiyor (aka com.gittigidiyormobil) application 1.4.1 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.   |
| Git | 2.45.2 | CVE-2014-8681 | None | None | SQL injection vulnerability in the GetIssues function in models/issue.go in Gogs (aka Go Git Service) 0.3.1-9 through 0.5.6.x before 0.5.6.1025 Beta allows remote attackers to execute arbitrary SQL commands via the label parameter to user/repos/issues.  |
| Git | 2.45.2 | CVE-2014-8682 | None | None | Multiple SQL injection vulnerabilities in Gogs (aka Go Git Service) 0.3.1-9 through 0.5.x before 0.5.6.1105 Beta allow remote attackers to execute arbitrary SQL commands via the q parameter to (1) api/v1/repos/search, which is not properly handled in models/repo.go, or (2) api/v1/users/search, which is not properly handled in models/user.go. |
| Git | 2.45.2 | CVE-2014-8683 | None | None | Cross-site scripting (XSS) vulnerability in models/issue.go in Gogs (aka Go Git Service) 0.3.1-9 through 0.5.x before 0.5.8 allows remote attackers to inject arbitrary web script or HTML via the text parameter to api/v1/markdown.   |
| Git | 2.45.2 | CVE-2013-4663 | None | None | git_http_controller.rb in the redmine_git_hosting plugin for Redmine allows remote attackers to execute arbitrary commands via shell metacharacters in (1) the service parameter to info/refs, related to the get_info_refs function or (2) the reqfile argument to the file_exists function.   |
| Git | 2.45.2 | CVE-2015-3903 | None | None | libraries/Config.class.php in phpMyAdmin 4.0.x before 4.0.10.10, 4.2.x before 4.2.13.3, 4.3.x before 4.3.13.1, and 4.4.x before 4.4.6.1 disables X.509 certificate verification for GitHub API calls over SSL, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.                    |

|     |        |               |          |      |   |
|-----|--------|---------------|----------|------|---|
| Git | 2.45.2 | CVE-2015-0850 | None     | None | The Git plugin for FusionForge before 6.0rc4 allows remote attackers to execute arbitrary code via an unspecified parameter when creating a secondary Git repository.   |
| Git | 2.45.2 | CVE-2015-7082 | None     | None | Multiple unspecified vulnerabilities in Git before 2.5.4, as used in Apple Xcode before 7.2, have unknown impact and attack vectors. NOTE: this CVE is associated only with Xcode use cases.  |
| Git | 2.45.2 | CVE-2016-2315 | CRITICAL | 9.8  | revision.c in git before 2.7.4 uses an incorrect integer data type, which allows remote attackers to execute arbitrary code via a (1) long filename or (2) many nested trees, leading to a heap-based buffer overflow.  |
| Git | 2.45.2 | CVE-2016-2324 | CRITICAL | 9.8  | Integer overflow in Git before 2.7.4 allows remote attackers to execute arbitrary code via a (1) long filename or (2) many nested trees, which triggers a heap-based buffer overflow.   |
| Git | 2.45.2 | CVE-2015-7545 | None     | None | The (1) git-remote-ext and (2) unspecified other remote helper programs in Git before 2.3.10, 2.4.x before 2.4.10, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 do not properly restrict the allowed protocols, which might allow remote attackers to execute arbitrary code via a URL in a (a) .gitmodules file or (b) unknown other sources in a submodule. |
| Git | 2.45.2 | CVE-2016-3068 | None     | None | Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted git ext:: URL when cloning a subrepository.  |
| Git | 2.45.2 | CVE-2016-3069 | None     | None | Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted name when converting a Git repository.   |
| Git | 2.45.2 | CVE-2016-3105 | None     | None | The convert extension in Mercurial before 3.8 might allow context-dependent attackers to execute arbitrary code via a crafted git repository name.  |
| Git | 2.45.2 | CVE-2016-2865 | None     | None | The GIT Integration component in IBM Rational Team Concert (RTC) 5.x before 5.0.2 iFix14 and 6.x before 6.0.1 iFix5 and Rational Collaborative Lifecycle Management 5.x before 5.0.2 iFix14 and 6.x before 6.0.1 iFix5 allows remote authenticated users to obtain sensitive information via a malformed request.   |

|     |        |                |          |      |  |
|-----|--------|----------------|----------|------|--|
| Git | 2.45.2 | CVE-2015-8968  | HIGH     | 8.8  | git-fastclone before 1.0.1 permits arbitrary shell command execution from .gitmodules. If an attacker can instruct a user to run a recursive clone from a repository they control, they can get a client to run an arbitrary shell command. Alternately, if an attacker can MITM an unencrypted git clone, they could exploit this. The ext command will be run if the repository is recursively cloned or if submodules are updated. This attack works when cloning both local and remote repositories.   |
| Git | 2.45.2 | CVE-2015-8969  | CRITICAL | 9.8  | git-fastclone before 1.0.5 passes user modifiable strings directly to a shell command. An attacker can execute malicious commands by modifying the strings that are passed as arguments to "cd " and " git clone " commands in the library.  |
| Git | 2.45.2 | CVE-2016-9086  | None     | None | GitLab versions 8.9.x and above contain a critical security flaw in the "import/export project" feature of GitLab. Added in GitLab 8.9, this feature allows a user to export and then re-import their projects as tape archive files (tar). All GitLab versions prior to 8.13.0 restricted this feature to administrators only. Starting with version 8.13.0 this feature was made available to all users. This feature did not properly check for symbolic links in user-provided archives and therefore it was possible for an authenticated user to retrieve the contents of any file accessible to the GitLab service account. This included sensitive files such as those that contain secret tokens used by the GitLab service to authenticate users. GitLab CE and EE versions 8.13.0 through 8.13.2, 8.12.0 through 8.12.7, 8.11.0 through 8.11.10, 8.10.0 through 8.10.12, and 8.9.0 through 8.9.11 are affected. |
| Git | 2.45.2 | CVE-2016-9274  | HIGH     | 7.8  | Untrusted search path vulnerability in Git 1.x for Windows allows local users to gain privileges via a Trojan horse git.exe file in the current working directory. NOTE: 2.x is unaffected.  |
| Git | 2.45.2 | CVE-2016-10075 | None     | None | The tqdm._version module in tqdm versions 4.4.1 and 4.10 allows local users to execute arbitrary code via a crafted repo with a malicious git log in the current working directory.  |
| Git | 2.45.2 | CVE-2016-7793  | None     | None | sociomantic-tsunami git-hub before 0.10.3 allows remote attackers to execute arbitrary code via a crafted repository URL.  |
| Git | 2.45.2 | CVE-2016-7794  | None     | None | sociomantic-tsunami git-hub before 0.10.3 allows remote attackers to execute arbitrary code via a crafted repository name.   |

|     |        |                |      |      |   |
|-----|--------|----------------|------|------|---|
| Git | 2.45.2 | CVE-2016-4340  | None | None | The impersonate feature in Gitlab 8.7.0, 8.6.0 through 8.6.7, 8.5.0 through 8.5.11, 8.4.0 through 8.4.9, 8.3.0 through 8.3.8, and 8.2.0 through 8.2.4 allows remote authenticated users to "log in" as any other user via unspecified vectors.  |
| Git | 2.45.2 | CVE-2016-8568  | None | None | The git_commit_message function in oid.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a cat-file command with a crafted object file.  |
| Git | 2.45.2 | CVE-2016-8569  | None | None | The git_oid_nfmt function in commit.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (NULL pointer dereference) via a cat-file command with a crafted object file.   |
| Git | 2.45.2 | CVE-2016-10026 | None | None | ikiwiki 3.20161219 does not properly check if a revision changes the access permissions for a page on sites with the git and recentchanges plugins and the CGI interface enabled, which allows remote attackers to revert certain changes by leveraging permissions to change the page before the revision was made.  |
| Git | 2.45.2 | CVE-2017-5972  | HIGH | 7.5  | The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumption) by sending many TCP SYN packets, as demonstrated by an attack against the kernel-3.10.0 package in CentOS Linux 7. NOTE: third parties have been unable to discern any relationship between the GitHub Engineering finding and the Trigemini.c attack code. |
| Git | 2.45.2 | CVE-2014-9938  | HIGH | 8.8  | contrib/completion/git-prompt.sh in Git before 1.9.3 does not sanitize branch names in the PS1 variable, allowing a malicious repository to cause code execution.   |
| Git | 2.45.2 | CVE-2016-10128 | None | None | Buffer overflow in the git_pkt_parse_line function in transports/smart_pkt.c in the Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to have unspecified impact via a crafted non-flush packet.   |
| Git | 2.45.2 | CVE-2016-10129 | None | None | The Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to cause a denial of service (NULL pointer dereference) via an empty packet line.  |

|     |        |               |      |      |   |
|-----|--------|---------------|------|------|---|
| Git | 2.45.2 | CVE-2016-9469 | None | None | Multiple versions of GitLab expose a dangerous method to any authenticated user that could lead to the deletion of all Issue and MergeRequest objects on a GitLab instance. For GitLab instances with publicly available projects this vulnerability could be exploited by an unauthenticated user. A fix was included in versions 8.14.3, 8.13.8, and 8.12.11, which were released on December 5th 2016 at 3:59 PST. The GitLab versions vulnerable to this are 8.13.0, 8.13.0-ee, 8.13.1, 8.13.1-ee, 8.13.2, 8.13.2-ee, 8.13.3, 8.13.3-ee, 8.13.4, 8.13.4-ee, 8.13.5, 8.13.5-ee, 8.13.6, 8.13.6-ee, 8.13.7, 8.14.0, 8.14.0-ee, 8.14.1, 8.14.2, and 8.14.2-ee. |
| Git | 2.45.2 | CVE-2017-0882 | None | None | Multiple versions of GitLab expose sensitive user credentials when assigning a user to an issue or merge request. A fix was included in versions 8.15.8, 8.16.7, and 8.17.4, which were released on March 20th 2017 at 23:59 UTC.   |
| Git | 2.45.2 | CVE-2017-5135 | None | None | Certain Technicolor devices have an SNMP access-control bypass, possibly involving an ISP customization in some cases. The Technicolor (formerly Cisco) DPC3928SL with firmware D3928SL-P15-13-A386-c3420r55105-160127a could be reached by any SNMP community string from the Internet; also, you can write in the MIB because it provides write properties, aka Stringbleed. NOTE: the string-bleed/StringBleed-CV E-2017-5135 GitHub repository is not a valid reference as of 2017-04-27; it contains Trojan horse code purported to exploit this vulnerability.  |
| Git | 2.45.2 | CVE-2017-8778 | None | None | GitLab before 8.14.9, 8.15.x before 8.15.6, and 8.16.x before 8.16.5 has XSS via a SCRIPT element in an issue attachment or avatar that is an SVG document.   |
| Git | 2.45.2 | CVE-2017-8833 | None | None | Zen Cart 1.6.0 has XSS in the main_page parameter to index.php. NOTE: 1.6.0 is not an official release but the vendor's README.md file offers a link to v160.zip with a description of "Download latest in-development version from github."  |
| Git | 2.45.2 | CVE-2017-8386 | None | None | git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.   |

|     |        |                |      |      |  |
|-----|--------|----------------|------|------|--|
| Git | 2.45.2 | CVE-2017-11353 | None | None | yadm (yet another dotfile manager) 1.10.0 has a race condition (related to the behavior of git commands in setting permissions for new files and directories), which potentially allows access to SSH and PGP keys.  |
| Git | 2.45.2 | CVE-2017-11437 | None | None | GitLab Enterprise Edition (EE) before 8.17.7, 9.0.11, 9.1.8, 9.2.8, and 9.3.8 allows an authenticated user with the ability to create a project to use the mirroring feature to potentially read repositories belonging to other users.  |
| Git | 2.45.2 | CVE-2017-11438 | None | None | GitLab Community Edition (CE) and Enterprise Edition (EE) before 9.0.11, 9.1.8, 9.2.8 allow an authenticated user with the ability to create a group to add themselves to any project that is inside a subgroup.   |
| Git | 2.45.2 | CVE-2017-12581 | None | None | GitHub Electron before 1.6.8 allows remote command execution because of a nodeIntegration bypass vulnerability. This also affects all applications that bundle Electron code equivalent to 1.6.8 or earlier. Bypassing the Same Origin Policy (SOP) is a precondition; however, recent Electron versions do not have strict SOP enforcement. Combining an SOP bypass with a privileged URL internally used by Electron, it was possible to execute native Node.js primitives in order to run OS commands on the user's host. Specifically, a chrome-devtools://devtools/bundled/inspector.html window could be used to eval a Node.js child_process.execFile API call. |
| Git | 2.45.2 | CVE-2017-12426 | None | None | GitLab Community Edition (CE) and Enterprise Edition (EE) before 8.17.8, 9.0.x before 9.0.13, 9.1.x before 9.1.10, 9.2.x before 9.2.10, 9.3.x before 9.3.10, and 9.4.x before 9.4.4 might allow remote attackers to execute arbitrary code via a crafted SSH URL in a project import.  |
| Git | 2.45.2 | CVE-2017-12963 | None | None | There is an illegal address access in Sass::Eval::operator() in eval.cpp of LibSass 3.4.5, leading to a remote denial of service attack. NOTE: this is similar to CVE-2017-11555 but remains exploitable after the vendor's CVE-2017-11555 fix (available from GitHub after 2017-07-24).   |
| Git | 2.45.2 | CVE-2017-12976 | None | None | git-annex before 6.20170818 allows remote attackers to execute arbitrary commands via an ssh URL with an initial dash character in the hostname, as demonstrated by an ssh://-eProxyCommand= URL, a related issue to CVE-2017-9800, CVE-2017-12836, CVE-2017-1000116, and CVE-2017-1000117.  |

|     |        |                      |      |      |   |
|-----|--------|----------------------|------|------|---|
| Git | 2.45.2 | CVE-2015-1395        | None | None | Directory traversal vulnerability in GNU patch versions which support Git-style patching before 2.7.3 allows remote attackers to write to arbitrary files with the permissions of the target user via a .. (dot dot) in a diff file name.   |
| Git | 2.45.2 | CVE-2014-8156        | None | None | The D-Bus security policy files in /etc/dbus-1/system.d/*.conf in fso-gsmd 0.12.0-3, fso-frameworkd 0.9.5.9+git20110512-4, and fso-usaged 0.12.0-2 as packaged in Debian, the upstream cornucopia.git (fsoaudiod, fsodatad, fsodeviced, fsogsmd, fsonetworkd, fsotdld, fsousaged) git master on 2015-01-19, the upstream framework.git 0.10.1 and git master on 2015-01-19, phonesod 0.1+git20121018-1 as packaged in Debian, Ubuntu and potentially other packages, and potentially other fso modules do not properly filter D-Bus message paths, which might allow local users to cause a denial of service (dbus-daemon memory consumption), or execute arbitrary code as root by sending a crafted D-Bus message to any D-Bus system service. |
| Git | 2.45.2 | CVE-2017-14867       | None | None | Git before 2.10.5, 2.11.x before 2.11.4, 2.12.x before 2.12.5, 2.13.x before 2.13.6, and 2.14.x before 2.14.2 uses unsafe Perl scripts to support subcommands such as cvsserver, which allows attackers to execute arbitrary OS commands via shell metacharacters in a module name. The vulnerable code is reachable via git-shell even without CVS support.  |
| Git | 2.45.2 | CVE-2017-100008<br>7 | None | None | GitHub Branch Source provides a list of applicable credential IDs to allow users configuring a job to select the one they'd like to use. This functionality did not check permissions, allowing any user with Overall/Read permission to get a list of valid credentials IDs. Those could be used as part of an attack to capture the credentials using another vulnerability.  |
| Git | 2.45.2 | CVE-2017-100009<br>1 | None | None | GitHub Branch Source Plugin connects to a user-specified GitHub API URL (e.g. GitHub Enterprise) as part of form validation and completion (e.g. to verify Scan Credentials are correct). This functionality improperly checked permissions, allowing any user with Overall/Read access to Jenkins to connect to any web server and send credentials with a known ID, thereby possibly capturing them. Additionally, this functionality did not require POST requests be used, thereby allowing the above to be performed without direct access to Jenkins via Cross-Site Request Forgery.  |

|     |        |                      |      |      |  |
|-----|--------|----------------------|------|------|--|
| Git | 2.45.2 | CVE-2017-100009<br>2 | None | None | Git Plugin connects to a user-specified Git repository as part of form validation. An attacker with no direct access to Jenkins but able to guess at a username/password credentials ID could trick a developer with job configuration permissions into following a link with a maliciously crafted Jenkins URL which would result in the Jenkins Git client sending the username and password to an attacker-controlled server.   |
| Git | 2.45.2 | CVE-2017-100010<br>6 | None | None | Blue Ocean allows the creation of GitHub organization folders that are set up to scan a GitHub organization for repositories and branches containing a Jenkinsfile, and create corresponding pipelines in Jenkins. Its SCM content REST API supports the pipeline creation and editing feature in Blue Ocean. The SCM content REST API did not check the current user's authentication or credentials. If the GitHub organization folder was created via Blue Ocean, it retained a reference to its creator's GitHub credentials. This allowed users with read access to the GitHub organization folder to create arbitrary commits in the repositories inside the GitHub organization corresponding to the GitHub organization folder with the GitHub credentials of the creator of the organization folder. Additionally, users with read access to the GitHub organization folder could read arbitrary file contents from the repositories inside the GitHub organization corresponding to the GitHub organization folder if the b... |
| Git | 2.45.2 | CVE-2017-100011<br>0 | None | None | Blue Ocean allows the creation of GitHub organization folders that are set up to scan a GitHub organization for repositories and branches containing a Jenkinsfile, and create corresponding pipelines in Jenkins. It did not properly check the current user's authentication and authorization when configuring existing GitHub organization folders. This allowed users with read access to the GitHub organization folder to reconfigure it, including changing the GitHub API endpoint for the organization folder to an attacker-controlled server to obtain the GitHub access token, if the organization folder was initially created using Blue Ocean.   |

|     |        |                      |          |      |   |
|-----|--------|----------------------|----------|------|---|
| Git | 2.45.2 | CVE-2017-15041       | CRITICAL | 9.8  | Go before 1.8.4 and 1.9.x before 1.9.1 allows "go get" remote command execution. Using custom domains, it is possible to arrange things so that example.com/pkg1 points to a Subversion repository but example.com/pkg1/pkg2 points to a Git repository. If the Subversion repository includes a Git checkout in its pkg2 directory and some other work is done to ensure the proper ordering of operations, "go get" can be tricked into reusing this Git checkout for the fetch of code from pkg2. If the Subversion repository's Git checkout has malicious commands in .git/hooks/, they will execute on the system running "go get." |
| Git | 2.45.2 | CVE-2015-6918        | None     | None | salt before 2015.5.5 leaks git usernames and passwords to the log.  |
| Git | 2.45.2 | CVE-2017-15298       | None     | None | Git through 2.14.2 mishandles layers of tree objects, which allows remote attackers to cause a denial of service (memory consumption) via a crafted repository, aka a Git bomb. This can also have an impact of disk consumption; however, an affected process typically would not survive its attempt to build the data structure in memory before writing to disk.  |
| Git | 2.45.2 | CVE-2017-15994       | None     | None | rsync 3.1.3-development before 2017-10-24 mishandles archaic checksums, which makes it easier for remote attackers to bypass intended access restrictions. NOTE: the rsync development branch has significant use beyond the rsync developers, e.g., the code has been copied for use in various GitHub projects.   |
| Git | 2.45.2 | CVE-2017-100024<br>2 | None     | None | Jenkins Git Client Plugin 2.4.2 and earlier creates temporary file with insecure permissions resulting in information disclosure  |
| Git | 2.45.2 | CVE-2017-16613       | None     | None | An issue was discovered in middleware.py in OpenStack Swauth through 1.2.0 when used with OpenStack Swift through 2.15.1. The Swift object store and proxy server are saving (unhashed) tokens retrieved from the Swauth middleware authentication mechanism to a log file as part of a GET URI. This allows attackers to bypass authentication by inserting a token into an X-Auth-Token header of a new request. NOTE: github.com/openstack/swauth URLs do not mean that Swauth is maintained by an official OpenStack project team.  |
| Git | 2.45.2 | CVE-2017-100021<br>4 | None     | None | GitPHP by xiphux is vulnerable to OS Command Injections   |

|     |        |                      |        |      |  |
|-----|--------|----------------------|--------|------|--|
| Git | 2.45.2 | CVE-2017-3738        | MEDIUM | 5.9  | There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to th... |
| Git | 2.45.2 | CVE-2017-17458       | None   | None | In Mercurial before 4.4.1, it is possible that a specially malformed repository can cause Git subrepositories to run arbitrary code in the form of a .git/hooks/post-update script checked into the repository. Typical use of Mercurial prevents construction of such repositories, but they can be created programmatically.   |
| Git | 2.45.2 | CVE-2017-17716       | None   | None | GitLab 9.4.x before 9.4.2 does not support LDAP SSL certificate verification, but a verify_certificates LDAP option was mentioned in the 9.4 release announcement. This issue occurred because code was not merged. This is related to use of the omniauth-ldap library and the gitlab_omniauth-ldap gem.  |
| Git | 2.45.2 | CVE-2017-17831       | None   | None | GitHub Git LFS before 2.1.1 allows remote attackers to execute arbitrary commands via an ssh URL with an initial dash character in the hostname, located on a "url =" line in a .lfsconfig file within a repository.   |
| Git | 2.45.2 | CVE-2017-100045<br>1 | None   | None | fs-git is a file system like api for git repository. The fs-git version 1.0.1 module relies on child_process.exec, however, the buildCommand method used to construct exec strings does not properly sanitize data and is vulnerable to command injection across all methods that use it and call exec.  |

|     |        |                      |      |      |   |
|-----|--------|----------------------|------|------|---|
| Git | 2.45.2 | CVE-2017-100045<br>5 | None | None | GuixSD prior to Git commit 5e66574a128937e7f2cf146d146225703ccfd5d used POSIX hard links incorrectly, leading the creation of setuid executables in "the store", violating a fundamental security assumption of GNU Guix.   |
| Git | 2.45.2 | CVE-2017-100042<br>4 | None | None | Github Electron version 1.6.4 - 1.6.11 and 1.7.0 - 1.7.5 is vulnerable to a URL Spoofing problem when opening PDFs in PDFium resulting loading arbitrary PDFs that a hacker can control.  |
| Git | 2.45.2 | CVE-2014-8540        | None | None | The groups API in GitLab 6.x and 7.x before 7.4.3 allows remote authenticated guest users to modify ownership of arbitrary groups by leveraging improper permission checks.   |
| Git | 2.45.2 | CVE-2018-5955        | None | None | An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields to the rest/user/ URI.  |
| Git | 2.45.2 | CVE-2018-100000<br>6 | None | None | GitHub Electron versions 1.8.2-beta.3 and earlier, 1.7.10 and earlier, 1.6.15 and earlier has a vulnerability in the protocol handler, specifically Electron apps running on Windows 10, 7 or 2008 that register custom protocol handlers can be tricked in arbitrary command execution if the user clicks on a specially crafted URL. This has been fixed in versions 1.8.2-beta.4, 1.7.11, and 1.6.16.  |
| Git | 2.45.2 | CVE-2017-14592       | None | None | Sourcetree for macOS had several argument and command injection bugs in Mercurial and Git repository handling. An attacker with permission to commit to a repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system. From version 1.4.0 of Sourcetree for macOS, this vulnerability can be triggered from a webpage through the use of the Sourcetree URI handler. Versions of Sourcetree for macOS starting with 1.0b2 before version 2.7.0 are affected by this vulnerability.             |
| Git | 2.45.2 | CVE-2017-14593       | None | None | Sourcetree for Windows had several argument and command injection bugs in Mercurial and Git repository handling. An attacker with permission to commit to a repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system. From version 0.8.4b of Sourcetree for Windows, this vulnerability can be triggered from a webpage through the use of the Sourcetree URI handler. Versions of Sourcetree for Windows starting with 0.5.1.0 before version 2.4.7.0 are affected by this vulnerability |

|     |        |                      |        |      |  |
|-----|--------|----------------------|--------|------|--|
| Git | 2.45.2 | CVE-2017-18036       | None   | None | The Github repository importer in Atlassian Bitbucket Server before version 5.3.0 allows remote attackers to determine if a service they could not otherwise reach has open ports via a Server Side Request Forgery (SSRF) vulnerability.  |
| Git | 2.45.2 | CVE-2017-18037       | None   | None | The git repository tag rest resource in Atlassian Bitbucket Server from version 3.7.0 before 4.14.11 (the fixed version for 4.14.x), from version 5.0.0 before 5.0.9 (the fixed version for 5.0.x), from version 5.1.0 before 5.1.8 (the fixed version for 5.1.x), from version 5.2.0 before 5.2.6 (the fixed version for 5.2.x), from version 5.3.0 before 5.3.4 (the fixed version for 5.3.x), from version 5.4.0 before 5.4.2 (the fixed version for 5.4.x), from version 5.5.0 before 5.5.1 (the fixed version for 5.5.x) and before 5.6.0 allows remote attackers to read arbitrary files via a path traversal vulnerability through the name of a git tag. |
| Git | 2.45.2 | CVE-2018-100002<br>1 | MEDIUM | 5.0  | GIT version 2.15.1 and earlier contains a Input Validation Error vulnerability in Client that can result in problems including messing up terminal configuration to RCE. This attack appear to be exploitable via The user must interact with a malicious git server, (or have their traffic modified in a MITM attack).   |
| Git | 2.45.2 | CVE-2018-7032        | None   | None | webcheckout in myrepos through 1.20171231 does not sanitize URLs that are passed to git clone, allowing a malicious website operator or a MitM attacker to take advantage of it for arbitrary code execution, as demonstrated by an "ext::sh -c" attack or an option injection attack.   |
| Git | 2.45.2 | CVE-2017-18087       | None   | None | The download commit resource in Atlassian Bitbucket Server from version 5.1.0 before version 5.1.7, from version 5.2.0 before version 5.2.5, from version 5.3.0 before version 5.3.3 and from version 5.4.0 before version 5.4.1 allows remote attackers to write files to disk potentially allowing them to gain code execution, exploit CVE-2017-1000117 if a vulnerable version of git is in use, and or determine if an internal service exists via an argument injection vulnerability in the at parameter.   |

|     |        |                  |      |      |  |
|-----|--------|------------------|------|------|--|
| Git | 2.45.2 | CVE-2018-7206    | HIGH | 8.8  | An issue was discovered in Project Jupyter JupyterHub OAuthenticator 0.6.x before 0.6.2 and 0.7.x before 0.7.3. When using JupyterHub with GitLab group whitelisting for access control, group membership was not checked correctly, allowing members not in the whitelisted groups to create accounts on the Hub. (Users were not allowed to access other users' accounts, but could create their own accounts on the Hub linked to their GitLab account. GitLab authentication not using gitlab_group_whitelist is unaffected. No other Authenticators are affected.)  |
| Git | 2.45.2 | CVE-2018-1000118 | None | None | Github Electron version Electron 1.8.2-beta.4 and earlier contains a Command Injection vulnerability in Protocol Handler that can result in command execute. This attack appear to be exploitable via the victim opening an electron protocol handler in their browser. This vulnerability appears to have been fixed in Electron 1.8.2-beta.5. This issue is due to an incomplete fix for CVE-2018-1000006, specifically the black list used was not case insensitive allowing an attacker to potentially bypass it.  |
| Git | 2.45.2 | CVE-2018-1000110 | None | None | An improper authorization vulnerability exists in Jenkins Git Plugin version 3.7.0 and earlier in GitStatus.java that allows an attacker with network access to obtain a list of nodes and users.  |
| Git | 2.45.2 | CVE-2018-1227    | None | None | Pivotal Concourse after 2018-03-05 might allow remote attackers to have an unspecified impact, if a customer obtained the Concourse software from a DNS domain that is no longer controlled by Pivotal. The original domain for the Concourse CI (concourse-dot-ci) open source project has been registered by an unknown actor, and is therefore no longer the official website for Concourse CI. The new official domain is concourse-ci.org. At approximately 4 am EDT on March 7, 2018 the Concourse OSS team began receiving reports that the Concourse domain was not responding. The Concourse OSS team discovered, upon investigation with both the original and the new domain registrars, that the originating domain registrar had made the domain available for purchase. This was done despite the domain being renewed by the Concourse OSS team through August 2018. For a customer to be affected, they would have needed to access a download from a "concourse-dot-ci" domain web site after March 6, 2018 18:00:00... |

|     |        |               |        |      |   |
|-----|--------|---------------|--------|------|---|
| Git | 2.45.2 | CVE-2018-8754 | MEDIUM | 5.5  | The libevt_record_values_read_event() function in libevt_record_values.c in libevt before 2018-03-17 does not properly check for out-of-bounds values of user SID data size, strings size, or data size. NOTE: the vendor has disputed this as described in libyal/libevt issue 5 on GitHub |
| Git | 2.45.2 | CVE-2017-0914 | None   | None | Gitlab Community and Enterprise Editions version 10.1, 10.2, and 10.2.4 are vulnerable to a SQL injection in the MilestoneFinder component resulting in disclosure of all data in a GitLab instance's database.   |
| Git | 2.45.2 | CVE-2017-0915 | None   | None | Gitlab Community Edition version 10.2.4 is vulnerable to a lack of input validation in the GitlabProjectsImportService resulting in remote code execution.  |
| Git | 2.45.2 | CVE-2017-0916 | None   | None | Gitlab Community Edition version 10.3 is vulnerable to a lack of input validation in the system_hook_push queue through web hook component resulting in remote code execution.  |
| Git | 2.45.2 | CVE-2017-0917 | None   | None | Gitlab Community Edition version 10.2.4 is vulnerable to lack of input validation in the CI job component resulting in persistent cross site scripting.   |
| Git | 2.45.2 | CVE-2017-0918 | None   | None | Gitlab Community Edition version 10.3 is vulnerable to a path traversal issue in the GitLab CI runner component resulting in remote code execution.   |
| Git | 2.45.2 | CVE-2017-0922 | None   | None | Gitlab Enterprise Edition version 10.3 is vulnerable to an authorization bypass issue in the GitLab Projects::BoardsController component resulting in an information disclosure on any board object.  |
| Git | 2.45.2 | CVE-2017-0923 | None   | None | Gitlab Community Edition version 9.1 is vulnerable to lack of input validation in the IPython notebooks component resulting in persistent cross site scripting.   |
| Git | 2.45.2 | CVE-2017-0924 | None   | None | Gitlab Community Edition version 10.2.4 is vulnerable to lack of input validation in the labels component resulting in persistent cross site scripting.   |
| Git | 2.45.2 | CVE-2017-0925 | None   | None | Gitlab Enterprise Edition version 10.1.0 is vulnerable to an insufficiently protected credential issue in the project service integration API endpoint resulting in an information disclosure of plaintext password.  |
| Git | 2.45.2 | CVE-2017-0926 | None   | None | Gitlab Community Edition version 10.3 is vulnerable to an improper authorization issue in the Oauth sign-in component resulting in unauthorized user login.   |

|     |        |                      |      |      |  |
|-----|--------|----------------------|------|------|--|
| Git | 2.45.2 | CVE-2017-0927        | None | None | Gitlab Community Edition version 10.3 is vulnerable to an improper authorization issue in the deployment keys component resulting in unauthorized use of deployment keys by guest users.   |
| Git | 2.45.2 | CVE-2018-3710        | HIGH | 7.8  | Gitlab Community and Enterprise Editions version 10.3.3 is vulnerable to an Insecure Temporary File in the project import component resulting remote code execution.   |
| Git | 2.45.2 | CVE-2017-0920        | None | None | GitLab Community and Enterprise Editions before 10.1.6, 10.2.6, and 10.3.4 are vulnerable to an authorization bypass issue in the Projects::MergeRequests::CreationsController component resulting in an attacker to see every project name and their respective namespace on a GitLab instance.   |
| Git | 2.45.2 | CVE-2018-8971        | None | None | The Auth0 integration in GitLab before 10.3.9, 10.4.x before 10.4.6, and 10.5.x before 10.5.6 has an incorrect omniauth-auth0 configuration, leading to signing in unintended users.   |
| Git | 2.45.2 | CVE-2016-6658        | None | None | Applications in cf-release before 245 can be configured and pushed with a user-provided custom buildpack using a URL pointing to the buildpack. Although it is not recommended, a user can specify a credential in the URL (basic auth or OAuth) to access the buildpack through the CLI. For example, the user could include a GitHub username and password in the URL to access a private repo. Because the URL to access the buildpack is stored unencrypted, an operator with privileged access to the Cloud Controller database could view these credentials. |
| Git | 2.45.2 | CVE-2018-100014<br>2 | None | None | An exposure of sensitive information vulnerability exists in Jenkins GitHub Pull Request Builder Plugin version 1.39.0 and older in GhprbCause.java that allows an attacker with local file system access to obtain GitHub credentials.  |
| Git | 2.45.2 | CVE-2018-100014<br>3 | None | None | An exposure of sensitive information vulnerability exists in Jenkins GitHub Pull Request Builder Plugin version 1.39.0 and older in GhprbCause.java that allows an attacker with local file system access to obtain GitHub credentials.  |
| Git | 2.45.2 | CVE-2018-9243        | None | None | GitLab Community and Enterprise Editions version 8.4 up to 10.4 are vulnerable to XSS because a lack of input validation in the merge request component leads to cross site scripting (specifically, filenames in changes tabs of merge requests). This is fixed in 10.6.3, 10.5.7, and 10.4.7.  |

|     |        |                  |      |      |   |
|-----|--------|------------------|------|------|---|
| Git | 2.45.2 | CVE-2018-9244    | None | None | GitLab Community and Enterprise Editions version 9.2 up to 10.4 are vulnerable to XSS because a lack of input validation in the milestones component leads to cross site scripting (specifically, data-milestone-id in the milestone dropdown feature). This is fixed in 10.6.3, 10.5.7, and 10.4.7.  |
| Git | 2.45.2 | CVE-2016-9645    | None | None | The fix for ikiwiki for CVE-2016-10026 was incomplete resulting in editing restriction bypass for git revert when using git versions older than 2.8.0. This has been fixed in 3.20161229.   |
| Git | 2.45.2 | CVE-2018-0023    | None | None | JSNAPy is an open source python version of Junos Snapshot Administrator developed by Juniper available through github. The default configuration and sample files of JSNAPy automation tool versions prior to 1.3.0 are created world writable. This insecure file and directory permission allows unprivileged local users to alter the files under this directory including inserting operations not intended by the package maintainer, system administrator, or other users. This issue only affects users who downloaded and installed JSNAPy from github. |
| Git | 2.45.2 | CVE-2018-1000160 | None | None | RisingStack protect version 1.2.0 and earlier contains a Cross Site Scripting (XSS) vulnerability in isXss() function in lib/rules/xss.js that can result in dangerous XSS strings being validated as safe. This attack appears to be exploitable via A number of XSS strings(26) detailed in the GitHub issue #16.   |
| Git | 2.45.2 | CVE-2018-8801    | None | None | GitLab Community and Enterprise Editions version 8.3 up to 10.x before 10.3 are vulnerable to SSRF in the Services and webhooks component.  |
| Git | 2.45.2 | CVE-2018-1000199 | None | None | The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() that can result in crash and possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to use ptrace. This vulnerability appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.   |
| Git | 2.45.2 | CVE-2018-11233   | None | None | In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, code to sanity-check pathnames on NTFS can result in reading out-of-bounds memory.  |

|     |        |                      |      |      |   |
|-----|--------|----------------------|------|------|---|
| Git | 2.45.2 | CVE-2018-11235       | None | None | In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, remote code execution can occur. With a crafted .gitmodules file, a malicious project can execute an arbitrary script on a machine that runs "git clone --recurse-submodules" because submodule "names" are obtained from this file, and then appended to \$GIT_DIR/modules, leading to directory traversal with "../" in a name. Finally, post-checkout hooks from a submodule are executed, bypassing the intended design in which hooks are not obtained from a remote server. |
| Git | 2.45.2 | CVE-2016-10526       | None | None | A common setup to deploy to gh-pages on every commit via a CI system is to expose a github token to ENV and to use it directly in the auth part of the url. In module versions < 0.9.1 the auth portion of the url is outputted as part of the grunt tasks logging function. If this output is publicly available then the credentials should be considered compromised.  |
| Git | 2.45.2 | CVE-2018-10379       | None | None | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 10.5.8, 10.6.x before 10.6.5, and 10.7.x before 10.7.2. The Move Issue feature contained a persistent XSS vulnerability.  |
| Git | 2.45.2 | CVE-2017-16019       | None | None | GitBook is a command line tool (and Node.js library) for building beautiful books using GitHub/Git and Markdown (or AsciiDoc). Stored Cross-Site-Scripting (XSS) is possible in GitBook before 3.2.2 by including code outside of backticks in any ebook. This code will be executed on the online reader.  |
| Git | 2.45.2 | CVE-2018-10813       | None | None | In Dedos-web 1.0, the cookie and session secrets used in the Express.js application have hardcoded values that are visible in the source code published on GitHub. An attacker can edit the contents of the session cookie and re-sign it using the hardcoded secret. Due to the use of Passport.js, this could lead to privilege escalation.   |
| Git | 2.45.2 | CVE-2018-100018<br>2 | None | None | A server-side request forgery vulnerability exists in Jenkins Git Plugin 3.9.0 and older in AssemblaWeb.java, GitBlitRepositoryBrowser.java, Gitiles.java, TFS2013GitRepositoryBrowser.java, ViewGitWeb.java that allows attackers with Overall/Read access to cause Jenkins to send a GET request to a specified URL.  |

|     |        |                      |      |      |   |
|-----|--------|----------------------|------|------|---|
| Git | 2.45.2 | CVE-2018-100018<br>3 | None | None | A exposure of sensitive information vulnerability exists in Jenkins GitHub Plugin 1.29.0 and older in GitHubServerConfig.java that allows attackers with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.                   |
| Git | 2.45.2 | CVE-2018-100018<br>4 | None | None | A server-side request forgery vulnerability exists in Jenkins GitHub Plugin 1.29.0 and older in GitHubPluginConfig.java that allows attackers with Overall/Read access to cause Jenkins to send a GET request to a specified URL.   |
| Git | 2.45.2 | CVE-2018-100018<br>5 | None | None | A server-side request forgery vulnerability exists in Jenkins GitHub Branch Source Plugin 2.3.4 and older in Endpoint.java that allows attackers with Overall/Read access to cause Jenkins to send a GET request to a specified URL.  |
| Git | 2.45.2 | CVE-2018-100018<br>6 | None | None | A exposure of sensitive information vulnerability exists in Jenkins GitHub Pull Request Builder Plugin 1.41.0 and older in GhprbGitHubAuth.java that allows attackers with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. |
| Git | 2.45.2 | CVE-2018-100019<br>6 | None | None | A exposure of sensitive information vulnerability exists in Jenkins Gitlab Hook Plugin 1.4.2 and older in gitlab_notifier.rb, views/gitlab_notifier/global.erb that allows attackers with local Jenkins master file system access or control of a Jenkins administrator's web browser (e.g. malicious extension) to retrieve the configured Gitlab token. |
| Git | 2.45.2 | CVE-2018-100020<br>3 | None | None | Soar Labs Soar Coin version up to and including git commit 4a2aa71ee21014e2880a3f7aad11091ed6ad434f (latest release as of Sept 2017) contains an intentional backdoor vulnerability in the function zero_fee_transaction() that can result in theft of Soar Coins by the "onlycentralAccount" (Soar Labs) after payment is processed.                     |
| Git | 2.45.2 | CVE-2017-16225       | None | None | aegir is a module to help automate JavaScript project management. Version 12.0.0 through and including 12.0.7 bundled and published to npm the user (that performed a aegir-release) GitHub token.  |

|     |        |                |        |      |  |
|-----|--------|----------------|--------|------|--|
| Git | 2.45.2 | CVE-2018-7559  | None   | None | An issue was discovered in OPC UA .NET Standard Stack and Sample Code before GitHub commit 2018-04-12, and OPC UA .NET Legacy Stack and Sample Code before GitHub commit 2018-03-13. A vulnerability in OPC UA applications can allow a remote attacker to determine a Server's private key by sending carefully constructed bad UserIdentityTokens as part of an oracle attack. |
| Git | 2.45.2 | CVE-2018-11723 | None   | None | The libpff_name_to_id_map_entry_read function in libpff_name_to_id_map.c in libyal libpff through 2018-04-28 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted pff file. NOTE: the vendor has disputed this as described in libyal/libpff issue 66 on GitHub  |
| Git | 2.45.2 | CVE-2018-11727 | MEDIUM | 5.5  | The libfsntfs_attribute_read_from_mft function in libfsntfs_attribute.c in libfsntfs through 2018-04-20 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted ntfs file. NOTE: the vendor has disputed this as described in libyal/libfsntfs issue 8 on GitHub  |
| Git | 2.45.2 | CVE-2018-11728 | MEDIUM | 5.5  | The libfsntfs_reparse_point_values_read_data function in libfsntfs_reparse_point_values.c in libfsntfs through 2018-04-20 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted ntfs file. NOTE: the vendor has disputed this as described in libyal/libfsntfs issue 8 on GitHub  |
| Git | 2.45.2 | CVE-2018-11729 | None   | None | The libfsntfs_mft_entry_read_header function in libfsntfs_mft_entry.c in libfsntfs through 2018-04-20 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted ntfs file. NOTE: the vendor has disputed this as described in libyal/libfsntfs issue 8 on GitHub  |
| Git | 2.45.2 | CVE-2018-11730 | None   | None | The libfsntfs_security_descriptor_values_free function in libfsntfs_security_descriptor_values.c in libfsntfs through 2018-04-20 allows remote attackers to cause a denial of service (double-free) via a crafted ntfs file. NOTE: the vendor has disputed this as described in libyal/libfsntfs issue 8 on GitHub   |
| Git | 2.45.2 | CVE-2018-11731 | None   | None | The libfsntfs_mft_entry_read_attributes function in libfsntfs_mft_entry.c in libfsntfs through 2018-04-20 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted ntfs file. NOTE: the vendor has disputed this as described in libyal/libfsntfs issue 8 on GitHub  |

|     |        |                      |          |      |   |
|-----|--------|----------------------|----------|------|---|
| Git | 2.45.2 | CVE-2018-12096       | None     | None | The liblnk_data_string_get_utf8_string_size function in liblnk_data_string.c in liblnk through 2018-04-19 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted lnk file. NOTE: the vendor has disputed this as described in libyal/liblnk issue 33 on GitHub  |
| Git | 2.45.2 | CVE-2018-12097       | None     | None | The liblnk_location_information_read_data function in liblnk_location_information.c in liblnk through 2018-04-19 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted lnk file. NOTE: the vendor has disputed this as described in libyal/liblnk issue 33 on GitHub   |
| Git | 2.45.2 | CVE-2018-12098       | None     | None | The liblnk_data_block_read function in liblnk_data_block.c in liblnk through 2018-04-19 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted lnk file. NOTE: the vendor has disputed this as described in libyal/liblnk issue 33 on GitHub  |
| Git | 2.45.2 | CVE-2018-100053<br>3 | CRITICAL | 9.8  | klauussilveira GitList version <= 0.6 contains a Passing incorrectly sanitized input to system function vulnerability in `searchTree` function that can result in Execute any code as PHP user. This attack appear to be exploitable via Send POST request using search form. This vulnerability appears to have been fixed in 0.7 after commit 87b8c26b023c3fc37f0796b14bb13710f397b322. |
| Git | 2.45.2 | CVE-2018-100060<br>0 | None     | None | A exposure of sensitive information vulnerability exists in Jenkins GitHub Plugin 1.29.1 and earlier in GitHubTokenCredentialsCreator.java that allows attackers to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.  |
| Git | 2.45.2 | CVE-2017-0919        | None     | None | GitLab Community and Enterprise Editions before 10.1.6, 10.2.6, and 10.3.4 are vulnerable to an authorization bypass issue in the GitLab import component resulting in an attacker being able to perform operations under a group in which they were previously unauthorized.   |
| Git | 2.45.2 | CVE-2017-0921        | None     | None | GitLab Community and Enterprise Editions before 10.1.6, 10.2.6, and 10.3.4 are vulnerable to an unverified password change issue in the PasswordsController component resulting in potential account takeover if a victim's session is compromised.   |

|     |        |                |        |      |  |
|-----|--------|----------------|--------|------|--|
| Git | 2.45.2 | CVE-2018-10887 | HIGH   | 8.1  | A flaw was found in libgit2 before version 0.27.3. It has been discovered that an unexpected sign extension in git_delta_apply function in delta.c file may lead to an integer overflow which in turn leads to an out of bound read, allowing to read before the base object. An attacker may use this flaw to leak memory addresses or cause a Denial of Service. |
| Git | 2.45.2 | CVE-2018-10888 | MEDIUM | 6.5  | A flaw was found in libgit2 before version 0.27.3. A missing check in git_delta_apply function in delta.c file, may lead to an out-of-bound read while reading a binary delta file. An attacker may use this flaw to cause a Denial of Service.  |
| Git | 2.45.2 | CVE-2018-10859 | None   | None | git-annex is vulnerable to an Information Exposure when decrypting files. A malicious server for a special remote could trick git-annex into decrypting a file that was encrypted to the user's gpg key. This attack could be used to expose encrypted data that was never stored in git-annex   |
| Git | 2.45.2 | CVE-2018-10857 | None   | None | git-annex is vulnerable to a private data exposure and exfiltration attack. It could expose the content of files located outside the git-annex repository, or content from a private web server on localhost or the LAN.   |
| Git | 2.45.2 | CVE-2018-14364 | None   | None | GitLab Community and Enterprise Edition before 10.7.7, 10.8.x before 10.8.6, and 11.x before 11.0.4 allows Directory Traversal with write access and resultant remote code execution via the GitLab projects import component.   |
| Git | 2.45.2 | CVE-2018-14601 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 11.1.x before 11.1.2. A Denial of Service can occur because Markdown rendering times are slow.  |
| Git | 2.45.2 | CVE-2018-14602 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. Information Disclosure can occur because the Prometheus metrics feature discloses private project pathnames.   |
| Git | 2.45.2 | CVE-2018-14603 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. CSRF can occur in the Test feature of the System Hooks component.  |
| Git | 2.45.2 | CVE-2018-14604 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur in the tooltip of the job inside the CI/CD pipeline.   |

|     |        |                |          |      |  |
|-----|--------|----------------|----------|------|--|
| Git | 2.45.2 | CVE-2018-14605 | None     | None | An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur in the branch name during a Web IDE file commit.   |
| Git | 2.45.2 | CVE-2018-14606 | None     | None | An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur via a Milestone name during a promotion.   |
| Git | 2.45.2 | CVE-2017-12148 | None     | None | A flaw was found in Ansible Tower's interface before 3.1.5 and 3.2.0 with SCM repositories. If a Tower project (SCM repository) definition does not have the 'delete before update' flag set, an attacker with commit access to the upstream playbook source repository could create a Trojan playbook that, when executed by Tower, modifies the checked out SCM repository to add git hooks. These git hooks could, in turn, cause arbitrary command and code execution as the user Tower runs as. |
| Git | 2.45.2 | CVE-2018-12605 | None     | None | An issue was discovered in GitLab Community Edition and Enterprise Edition 10.7.x before 10.7.6. The usage of 'url_for' contained a XSS issue due to it allowing arbitrary protocols as a parameter.   |
| Git | 2.45.2 | CVE-2018-12606 | None     | None | An issue was discovered in GitLab Community Edition and Enterprise Edition before 10.7.6, 10.8.x before 10.8.5, and 11.x before 11.0.1. The wiki contains a persistent XSS issue due to a lack of output encoding affecting a specific markdown feature.   |
| Git | 2.45.2 | CVE-2018-12607 | None     | None | An issue was discovered in GitLab Community Edition and Enterprise Edition before 10.7.6, 10.8.x before 10.8.5, and 11.x before 11.0.1. The charts feature contained a persistent XSS issue due to a lack of output encoding.  |
| Git | 2.45.2 | CVE-2018-15192 | None     | None | An SSRF vulnerability in webhooks in Gitea through 1.5.0-rc2 and Gogs through 0.11.53 allows remote attackers to access intranet services.   |
| Git | 2.45.2 | CVE-2018-3785  | CRITICAL | 9.8  | A command injection in git-dummy-commit v1.3.0 allows os level commands to be executed due to an unescaped parameter.  |
| Git | 2.45.2 | CVE-2018-15685 | None     | None | GitHub Electron 1.7.15, 1.8.7, 2.0.7, and 3.0.0-beta.6, in certain scenarios involving IFRAME elements and "nativeWindowOpen: true" or "sandbox: true" options, is affected by a WebPreferences vulnerability that can be leveraged to perform remote code execution.  |

|     |        |                |      |      |  |
|-----|--------|----------------|------|------|--|
| Git | 2.45.2 | CVE-2018-15157 | None | None | The libfscifs_block_read function in libfscifs_block.c in libfscifs before 2018-07-25 allows remote attackers to cause a heap-based buffer over-read via a crafted cifs file. NOTE: the vendor has disputed this as described in the GitHub issue comments                                   |
| Git | 2.45.2 | CVE-2018-15158 | None | None | The libesedb_page_read_values function in libesedb_page.c in libesedb through 2018-04-01 allows remote attackers to cause a heap-based buffer over-read via a crafted esedb file. NOTE: the vendor has disputed this as described in the GitHub issue comments                               |
| Git | 2.45.2 | CVE-2018-15159 | None | None | The libesedb_page_read_tags function in libesedb_page.c in libesedb through 2018-04-01 allows remote attackers to cause a heap-based buffer over-read via a crafted esedb file. NOTE: the vendor has disputed this as described in the GitHub issue comments                                 |
| Git | 2.45.2 | CVE-2018-15160 | None | None | The libesedb_catalog_definition_read function in libesedb_catalog_definition.c in libesedb through 2018-04-01 allows remote attackers to cause a heap-based buffer over-read via a crafted esedb file. NOTE: the vendor has disputed this as described in the GitHub issue comments          |
| Git | 2.45.2 | CVE-2018-15161 | None | None | The libesedb_key_append_data function in libesedb_key.c in libesedb through 2018-04-01 allows remote attackers to cause a heap-based buffer over-read via a crafted esedb file. NOTE: the vendor has disputed this as described in the GitHub issue comments                                 |
| Git | 2.45.2 | CVE-2018-16976 | None | None | Gitolite before 3.6.9 does not (in certain configurations involving @all or a regex) properly restrict access to a Git repository that is in the process of being migrated until the full set of migration steps has been completed. This can allow valid users to obtain unintended access. |
| Git | 2.45.2 | CVE-2013-4451  | None | None | gitolite commit fa06a34 through 3.5.3 might allow attackers to have unspecified impact via vectors involving world-writable permissions when creating (1) ~/.gitolite.rc, (2) ~/.gitolite, or (3) ~/repositories/gitolite-admin.git on fresh installs.                                       |
| Git | 2.45.2 | CVE-2013-7203  | None | None | gitolite before commit fa06a34 might allow local users to read arbitrary files in repositories via vectors related to the user umask when running gitolite setup.  |

|     |        |                      |      |      |  |
|-----|--------|----------------------|------|------|--|
| Git | 2.45.2 | CVE-2018-16048       | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.0.6, 11.1.x before 11.1.5, and 11.2.x before 11.2.2. There is Missing Authorization Control for API Repository Storage.   |
| Git | 2.45.2 | CVE-2018-16049       | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.0.6, 11.1.x before 11.1.5, and 11.2.x before 11.2.2. There is Sensitive Data Disclosure in Sidekiq Logs through an Error Message.   |
| Git | 2.45.2 | CVE-2018-16050       | None | None | An issue was discovered in GitLab Community and Enterprise Edition 11.1.x before 11.1.5 and 11.2.x before 11.2.2. There is Persistent XSS in the Merge Request Changes View.   |
| Git | 2.45.2 | CVE-2018-16051       | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.0.6, 11.1.x before 11.1.5, and 11.2.x before 11.2.2. There is Orphaned Upload Files Exposure.   |
| Git | 2.45.2 | CVE-2018-17456       | None | None | Git before 2.14.5, 2.15.x before 2.15.3, 2.16.x before 2.16.5, 2.17.x before 2.17.2, 2.18.x before 2.18.1, and 2.19.x before 2.19.1 allows remote code execution during processing of a recursive "git clone" of a superproject if a .gitmodules file has a URL field beginning with a '-' character.  |
| Git | 2.45.2 | CVE-2018-100080<br>3 | None | None | Gitea version prior to version 1.5.1 contains a CWE-200 vulnerability that can result in Exposure of users private email addresses. This attack appear to be exploitable via Watch a repository to receive email notifications. Emails received contain the other recipients even if they have the email set as private. This vulnerability appears to have been fixed in 1.5.1. |
| Git | 2.45.2 | CVE-2018-18926       | None | None | Gitea before 1.5.4 allows remote code execution because it does not properly validate session IDs. This is related to session ID handling in the go-macaron/session code for Macaron.  |
| Git | 2.45.2 | CVE-2018-13396       | None | None | There was an argument injection vulnerability in Sourcetree for macOS from version 1.0b2 before version 3.0.0 via Git subrepositories in Mercurial repositories. An attacker with permission to commit to a Mercurial repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system.  |

|     |        |                |      |      |   |
|-----|--------|----------------|------|------|---|
| Git | 2.45.2 | CVE-2018-13397 | None | None | There was an argument injection vulnerability in Sourcetree for Windows from version 0.5.1.0 before version 3.0.0 via Git subrepositories in Mercurial repositories. An attacker with permission to commit to a Mercurial repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system. |
| Git | 2.45.2 | CVE-2018-19486 | None | None | Git before 2.19.2 on Linux and UNIX executes commands from the current working directory (as if ' .' were at the end of \$PATH) in certain cases involving the run_command() API and run-command.c, because there was a dangerous change from execvp to execv during 2017.  |
| Git | 2.45.2 | CVE-2018-18649 | None | None | An issue was discovered in the wiki API in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It allows for remote code execution.  |
| Git | 2.45.2 | CVE-2018-17939 | None | None | An issue was discovered in GitLab Community and Enterprise Edition 11.1.x before 11.1.8, 11.2.x before 11.2.5, and 11.3.x before 11.3.2. There is Information Exposure via the merge request JSON endpoint.   |
| Git | 2.45.2 | CVE-2018-17975 | None | None | An issue was discovered in GitLab Community Edition 11.x before 11.1.8, 11.2.x before 11.2.5, and 11.3.x before 11.3.2. There is Information Exposure via the GFM markdown API.   |
| Git | 2.45.2 | CVE-2018-17976 | None | None | An issue was discovered in GitLab Community Edition 11.x before 11.1.8, 11.2.x before 11.2.5, and 11.3.x before 11.3.2. There is Information Exposure via Epic change descriptions.   |
| Git | 2.45.2 | CVE-2018-18640 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It has Information Exposure Through Browser Caching.  |
| Git | 2.45.2 | CVE-2018-18641 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It has Cleartext Storage of Sensitive Information.  |
| Git | 2.45.2 | CVE-2018-18642 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It has XSS.   |
| Git | 2.45.2 | CVE-2018-18644 | None | None | An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It allows Information Exposure via a Gitlab Prometheus integration.  |

|     |        |                |      |      |  |
|-----|--------|----------------|------|------|--|
| Git | 2.45.2 | CVE-2018-18645 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It allows for Information Exposure via unsubscribe links in email replies.   |
| Git | 2.45.2 | CVE-2018-18646 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It allows SSRF.  |
| Git | 2.45.2 | CVE-2018-18647 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It has Missing Authorization.  |
| Git | 2.45.2 | CVE-2018-18648 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It has Information Exposure Through an Error Message.  |
| Git | 2.45.2 | CVE-2018-18843 | None | None | The Kubernetes integration in GitLab Enterprise Edition 11.x before 11.2.8, 11.3.x before 11.3.9, and 11.4.x before 11.4.4 has SSRF.   |
| Git | 2.45.2 | CVE-2018-16873 | HIGH | 8.1  | In Go before 1.10.6 and 1.11.x before 1.11.3, the "go get" command is vulnerable to remote code execution when executed with the -u flag and the import path of a malicious Go package, or a package that imports it directly or indirectly. Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at <a href="https://golang.org/cmd/go/#hdr-Module_aware_go_get">https://golang.org/cmd/go/#hdr-Module_aware_go_get</a> ). Using custom domains, it's possible to arrange things so that a Git repository is cloned to a folder named ".git" by using a vanity import path that ends with "/.git". If the Git repository root contains a "HEAD" file, a "config" file, an "objects" directory, a "refs" directory, with some work to ensure the proper ordering of operations, "go get -u" can be tricked into considering the parent directory as a repository root, and running Git commands on it. That will use the "config" file in the original Git repository root for its configuration, and if that config file contains malicious comma... |

|     |        |                      |        |      |   |
|-----|--------|----------------------|--------|------|---|
| Git | 2.45.2 | CVE-2018-20167       | None   | None | Terminology before 1.3.1 allows Remote Code Execution because popmedia is mishandled, as demonstrated by an unsafe "cat README.md" command when \e}pn is used. A popmedia control sequence can allow the malicious execution of executable file formats registered in the X desktop share MIME types (/usr/share/applications). The control sequence defers unknown file types to the handle_unknown_media() function, which executes xdg-open against the filename specified in the sequence. The use of xdg-open for all unknown file types allows executable file formats with a registered shared MIME type to be executed. An attacker can achieve remote code execution by introducing an executable file and a plain text file containing the control sequence through a fake software project (e.g., in Git or a tarball). When the control sequence is rendered (such as with cat), the executable file will be run. |
| Git | 2.45.2 | CVE-2018-100084<br>3 | None   | None | Luigi version prior to version 2.8.0; after commit 53b52e12745075a8acc016d33945d9d6a7a6aaeb; after GitHub PR spotify/luigi/pull/1870 contains a Cross site Request Forgery (CSRF) vulnerability in API endpoint: /api/<method> that can result in Task metadata such as task name, id, parameter, etc. will be leaked to unauthorized users. This attack appear to be exploitable via The victim must visit a specially crafted webpage from the network where their Luigi server is accessible.. This vulnerability appears to have been fixed in 2.8.0 and later.   |
| Git | 2.45.2 | CVE-2018-100042<br>6 | MEDIUM | 6.1  | A cross-site scripting vulnerability exists in Jenkins Git Changelog Plugin 2.6 and earlier in GitChangelogSummaryDecorator/summary.jelly, GitChangelogLeftsideBuildDecorator/badge.jelly, GitLogJiraFilterPostPublisher/config.jelly, GitLogBasicChangelogPostPublisher/config.jelly that allows attackers able to control the Git history parsed by the plugin to have Jenkins render arbitrary HTML on some pages.   |
| Git | 2.45.2 | CVE-2018-20683       | None   | None | commands/rsync in Gitolite before 3.6.11, if .gitolite.rc enables rsync, mishandles the rsync command line, which allows attackers to have a "bad" impact by triggering use of an option other than -v, -n, -q, or -P.  |

|     |        |                  |          |      |   |
|-----|--------|------------------|----------|------|---|
| Git | 2.45.2 | CVE-2019-1000002 | None     | None | Gitea version 1.6.2 and earlier contains a Incorrect Access Control vulnerability in Delete/Edit file functionality that can result in the attacker deleting files outside the repository he/she has access to. This attack appears to be exploitable via the attacker must get write access to "any" repository including self-created ones.. This vulnerability appears to have been fixed in 1.6.3, 1.7.0-rc2. |
| Git | 2.45.2 | CVE-2019-1003010 | None     | None | A cross-site request forgery vulnerability exists in Jenkins Git Plugin 3.9.1 and earlier in src/main/java/hudson/plugins/git/GitTagAction.java that allows attackers to create a Git tag in a workspace and attach corresponding metadata to a build record.   |
| Git | 2.45.2 | CVE-2019-1003018 | None     | None | An exposure of sensitive information vulnerability exists in Jenkins GitHub Authentication Plugin 0.29 and earlier in GithubSecurityRealm/config.jelly that allows attackers able to view a Jenkins administrator's web browser output, or control the browser (e.g. malicious extension) to retrieve the configured client secret.   |
| Git | 2.45.2 | CVE-2019-1003019 | None     | None | An session fixation vulnerability exists in Jenkins GitHub Authentication Plugin 0.29 and earlier in GithubSecurityRealm.java that allows unauthorized attackers to impersonate another user if they can control the pre-authentication session.  |
| Git | 2.45.2 | CVE-2019-4059    | CRITICAL | 9.8  | IBM Rational ClearCase 1.0.0.0 GIT connector does not sufficiently protect the document database password. An attacker could obtain the password and gain unauthorized access to the document database. IBM X-Force ID: 156583.   |
| Git | 2.45.2 | CVE-2019-5917    | None     | None | azure-umqtt-c (available through GitHub prior to 2017 October 6) allows remote attackers to cause a denial of service via unspecified vectors.  |
| Git | 2.45.2 | CVE-2019-9785    | None     | None | gitnote 3.1.0 allows remote attackers to execute arbitrary code via a crafted Markdown file, as demonstrated by a javascript:window.parent.top.require('child_process').execFile substring in the onerror attribute of an IMG element.  |
| Git | 2.45.2 | CVE-2019-6240    | None     | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.4. It allows Directory Traversal.  |
| Git | 2.45.2 | CVE-2018-19856   | None     | None | GitLab CE/EE before 11.3.12, 11.4.x before 11.4.10, and 11.5.x before 11.5.3 allows Directory Traversal in Templates API.   |

|     |        |                |      |      |   |
|-----|--------|----------------|------|------|---|
| Git | 2.45.2 | CVE-2017-18365 | None | None | The Management Console in GitHub Enterprise 2.8.x before 2.8.7 has a deserialization issue that allows unauthenticated remote attackers to execute arbitrary code. This occurs because the enterprise session secret is always the same, and can be found in the product's source code. By sending a crafted cookie signed with this secret, one can call Marshal.load with arbitrary data, which is a problem because the Marshal data format allows Ruby objects. |
| Git | 2.45.2 | CVE-2018-20144 | None | None | GitLab Community and Enterprise Edition 11.x before 11.3.13, 11.4.x before 11.4.11, and 11.5.x before 11.5.4 has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2018-20229 | None | None | GitLab Community and Enterprise Edition before 11.3.14, 11.4.x before 11.4.12, and 11.5.x before 11.5.5 allows Directory Traversal.   |
| Git | 2.45.2 | CVE-2019-6796  | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows XSS (issue 2 of 2). The user status field contains a lack of input validation and output encoding that results in a persistent XSS.   |
| Git | 2.45.2 | CVE-2019-11228 | None | None | repo/setting.go in Gitea before 1.7.6 and 1.8.x before 1.8-RC3 does not validate the form.MirrorAddress before calling SaveAddress.   |
| Git | 2.45.2 | CVE-2019-11229 | HIGH | 8.8  | models/repo_mirror.go in Gitea before 1.7.6 and 1.8.x before 1.8-RC3 mishandles mirror repo URL settings, leading to remote code execution.   |
| Git | 2.45.2 | CVE-2019-7155  | None | None | An issue was discovered in GitLab Community and Enterprise Edition 9.x, 10.x, and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. A user retains their role within a project in a private group after being removed from the group, if their privileges within the project are different from the group.   |
| Git | 2.45.2 | CVE-2019-9170  | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2019-9171  | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 1 of 5).   |
| Git | 2.45.2 | CVE-2019-9172  | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 2 of 5).   |

|     |        |               |      |      |  |
|-----|--------|---------------|------|------|--|
| Git | 2.45.2 | CVE-2019-9174 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows SSRF.   |
| Git | 2.45.2 | CVE-2019-9175 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 3 of 5).                      |
| Git | 2.45.2 | CVE-2019-9176 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows CSRF.   |
| Git | 2.45.2 | CVE-2019-9178 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 4 of 5).                      |
| Git | 2.45.2 | CVE-2019-9179 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 5 of 5).                      |
| Git | 2.45.2 | CVE-2019-9217 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. Its User Interface has a Misrepresentation of Critical Information. |
| Git | 2.45.2 | CVE-2019-9219 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 2 of 5).                     |
| Git | 2.45.2 | CVE-2019-9220 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Uncontrolled Resource Consumption.                        |
| Git | 2.45.2 | CVE-2019-9222 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-9223 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure.                                     |
| Git | 2.45.2 | CVE-2019-9224 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 4 of 5).                     |
| Git | 2.45.2 | CVE-2019-9225 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 5 of 5).                     |

|     |        |                |        |      |  |
|-----|--------|----------------|--------|------|--|
| Git | 2.45.2 | CVE-2019-9756  | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting from 10.8) and 11.x before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control, a different vulnerability than CVE-2019-9732.   |
| Git | 2.45.2 | CVE-2019-9890  | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-10300 | None   | None | A cross-site request forgery vulnerability in Jenkins GitLab Plugin 1.5.11 and earlier in the GitLabConnectionConfig#doTestConnection form validation method allowed attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.                        |
| Git | 2.45.2 | CVE-2019-10301 | HIGH   | 8.8  | A missing permission check in Jenkins GitLab Plugin 1.5.11 and earlier in the GitLabConnectionConfig#doTestConnection form validation method allowed attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.           |
| Git | 2.45.2 | CVE-2019-11463 | MEDIUM | 5.5  | A memory leak in archive_read_format_zip_cleanup in archive_read_support_format_zip.c in libarchive 3.3.4-dev allows remote attackers to cause a denial of service via a crafted ZIP file because of a HAVE_LZMA_H typo. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected. |
| Git | 2.45.2 | CVE-2019-11217 | None   | None | The GitController in Jakub Chodounsky Bonobo Git Server before 6.5.0 allows execution of arbitrary commands in the context of the web server via a crafted http request.   |
| Git | 2.45.2 | CVE-2019-11218 | None   | None | Improper handling of extra parameters in the AccountController (User Profile edit) in Jakub Chodounsky Bonobo Git Server before 6.5.0 allows authenticated users to gain application administrator privileges via additional form parameter submissions.   |
| Git | 2.45.2 | CVE-2018-18643 | None   | None | GitLab CE & EE 11.2 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 have Persistent XSS.   |
| Git | 2.45.2 | CVE-2018-19359 | None   | None | GitLab Community and Enterprise Edition 8.9 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 has Incorrect Access Control.  |

|     |        |                |        |      |   |
|-----|--------|----------------|--------|------|---|
| Git | 2.45.2 | CVE-2019-11576 | None   | None | Gitea before 1.8.0 allows 1FA for user accounts that have completed 2FA enrollment. If a user's credentials are known, then an attacker could send them to the API without requiring the 2FA one-time password.   |
| Git | 2.45.2 | CVE-2019-10315 | None   | None | Jenkins GitHub Authentication Plugin 0.31 and earlier did not use the state parameter of OAuth to prevent CSRF.   |
| Git | 2.45.2 | CVE-2019-11000 | MEDIUM | 6.5  | An issue was discovered in GitLab Enterprise Edition before 11.7.11, 11.8.x before 11.8.7, and 11.9.x before 11.9.7. It allows Information Disclosure.  |
| Git | 2.45.2 | CVE-2019-10640 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.7.10, 11.8.x before 11.8.6, and 11.9.x before 11.9.4. A regex input validation issue for the .gitlab-ci.yml refs value allows Uncontrolled Resource Consumption.   |
| Git | 2.45.2 | CVE-2019-10108 | None   | None | An Incorrect Access Control (issue 1 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. It allowed non-members of a private project/group to add and read labels.   |
| Git | 2.45.2 | CVE-2019-10109 | None   | None | An Information Exposure issue (issue 1 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. EXIF geolocation data were not removed from images when uploaded to GitLab. As a result, anyone with access to the uploaded image could obtain its geolocation, device, and software version data (if present). |
| Git | 2.45.2 | CVE-2019-10110 | None   | None | An Insecure Permissions issue (issue 1 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The "move issue" feature may allow a user to create projects under any namespace on any GitLab instance on which they hold credentials.   |
| Git | 2.45.2 | CVE-2019-10111 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. It allows persistent XSS in the merge request "resolve conflicts" page.   |
| Git | 2.45.2 | CVE-2019-10113 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/<id>/languages requests may allow Uncontrolled Resource Consumption.   |

|     |        |                |      |      |  |
|-----|--------|----------------|------|------|--|
| Git | 2.45.2 | CVE-2019-10114 | None | None | An Information Exposure issue (issue 2 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. During the OAuth authentication process, the application attempts to validate a parameter in an insecure way, potentially exposing data.                                 |
| Git | 2.45.2 | CVE-2019-10115 | None | None | An Insecure Permissions issue (issue 2 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The GitLab Releases feature could allow guest users access to private information like release details and code information.   |
| Git | 2.45.2 | CVE-2019-10116 | None | None | An Insecure Permissions issue (issue 3 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. Guests of a project were allowed to see Related Branches created for an issue.   |
| Git | 2.45.2 | CVE-2019-10117 | None | None | An Open Redirect issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. A redirect is triggered after successful authentication within the OAuth::GeoAuthController for the secondary Geo node.  |
| Git | 2.45.2 | CVE-2019-10112 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The construction of the HMAC key was insecurely derived.   |
| Git | 2.45.2 | CVE-2018-19585 | None | None | GitLab CE/EE versions 8.18 up to 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1 have CRLF Injection in Project Mirroring when using the Git protocol.   |
| Git | 2.45.2 | CVE-2018-20500 | None | None | An insecure permissions issue was discovered in GitLab Community and Enterprise Edition 9.4 and later but before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. The runner registration token in the CI/CD settings could not be reset. This was a security risk if one of the maintainers leaves the group and they know the token. |
| Git | 2.45.2 | CVE-2019-5883  | None | None | An Incorrect Access Control issue was discovered in GitLab Community and Enterprise Edition 6.0 and later but before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. The issue comments feature could allow a user to comment on an issue which they shouldn't be allowed to.   |

|     |        |               |      |      |   |
|-----|--------|---------------|------|------|---|
| Git | 2.45.2 | CVE-2019-6781 | HIGH | 7.5  | An Improper Input Validation issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It was possible to use the profile name to inject a potentially malicious link into notification emails.  |
| Git | 2.45.2 | CVE-2019-6787 | None | None | An Incorrect Access Control issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The GitLab API allowed project Maintainers and Owners to view the trigger tokens of other project users.   |
| Git | 2.45.2 | CVE-2019-6790 | None | None | An Incorrect Access Control (issue 2 of 3) issue was discovered in GitLab Community and Enterprise Edition 8.14 and later but before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. Guest users were able to view the list of a group's merge requests.  |
| Git | 2.45.2 | CVE-2019-6797 | None | None | An information disclosure issue was discovered in GitLab Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The GitHub token used in CI/CD for External Repos was being leaked to project maintainers in the UI.   |
| Git | 2.45.2 | CVE-2019-7353 | None | None | An Incorrect Access Control issue was discovered in GitLab Community and Enterprise Edition 11.7.x before 11.7.4. GitLab Releases were vulnerable to an authorization issue that allowed users to view confidential issue and merge request titles of other projects.                                       |
| Git | 2.45.2 | CVE-2019-7549 | None | None | An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.5.10, 11.6.x before 11.6.8, and 11.7.x before 11.7.3. It has Incorrect Access Control. The GitLab pipelines feature is vulnerable to authorization issues that allow unauthorized users to view job information. |
| Git | 2.45.2 | CVE-2019-9218 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 1 of 5).  |
| Git | 2.45.2 | CVE-2019-9221 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 3 of 5).  |
| Git | 2.45.2 | CVE-2019-9485 | None | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.   |

|     |        |                |        |      |   |
|-----|--------|----------------|--------|------|---|
| Git | 2.45.2 | CVE-2019-9732  | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting from 10.8) and 11.x before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-9866  | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.7.7 and 11.8.x before 11.8.3. It allows Information Disclosure.   |
| Git | 2.45.2 | CVE-2019-10330 | HIGH   | 7.5  | Jenkins Gitea Plugin 1.1.1 and earlier did not implement trusted revisions, allowing attackers without commit access to the Git repo to change Jenkinsfiles even if Jenkins is configured to consider them to be untrusted.   |
| Git | 2.45.2 | CVE-2018-19493 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is a persistent XSS vulnerability in the environment pages due to a lack of input validation and output encoding.   |
| Git | 2.45.2 | CVE-2018-19494 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access vulnerability that allows an unauthorized user to view private group names.  |
| Git | 2.45.2 | CVE-2018-19495 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an SSRF vulnerability in the Prometheus integration.  |
| Git | 2.45.2 | CVE-2018-19496 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access control vulnerability that permits a user with insufficient privileges to promote a project milestone to a group milestone. |
| Git | 2.45.2 | CVE-2018-19577 | MEDIUM | 5.3  | Gitlab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an incorrect access control vulnerability that displays to an unauthorized user the title and namespace of a confidential issue.  |
| Git | 2.45.2 | CVE-2018-19569 | None   | None | GitLab CE/EE, versions 8.8 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an authorization vulnerability that allows access to the web-UI as a user using a Personal Access Token of any scope.   |
| Git | 2.45.2 | CVE-2018-19570 | MEDIUM | 5.4  | GitLab CE/EE, versions 11.3 before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via unrecognized HTML tags.   |

|     |        |                |        |      |  |
|-----|--------|----------------|--------|------|--|
| Git | 2.45.2 | CVE-2018-19572 | None   | None | GitLab CE 8.17 and later and EE 8.3 and later have a symlink time-of-check-to-time-of-use race condition that would allow unauthorized access to files in the GitLab Pages chroot environment. This is fixed in versions 11.5.1, 11.4.8, and 11.3.11.                    |
| Git | 2.45.2 | CVE-2018-19573 | MEDIUM | 5.4  | GitLab CE/EE, versions 10.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via Mermaid.  |
| Git | 2.45.2 | CVE-2018-19574 | MEDIUM | 5.4  | GitLab CE/EE, versions 7.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in the OAuth authorization page.  |
| Git | 2.45.2 | CVE-2018-19575 | None   | None | GitLab CE/EE, versions 10.1 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an insecure direct object reference issue that allows a user to make comments on a locked issue.  |
| Git | 2.45.2 | CVE-2018-19576 | None   | None | GitLab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an access control issue that allows a Guest user to make changes to or delete their own comments on an issue, after the issue was made Confidential. |
| Git | 2.45.2 | CVE-2018-19571 | HIGH   | 7.7  | GitLab CE/EE, versions 8.18 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an SSRF vulnerability in webhooks.  |
| Git | 2.45.2 | CVE-2018-19578 | None   | None | GitLab EE, version 11.5 before 11.5.1, is vulnerable to an insecure object reference issue that permits a user with Reporter privileges to view the Jaeger Tracing Operations page.  |
| Git | 2.45.2 | CVE-2018-19579 | None   | None | GitLab EE version 11.5 is vulnerable to a persistent XSS vulnerability in the Operations page. This is fixed in 11.5.1.  |
| Git | 2.45.2 | CVE-2018-19580 | None   | None | All versions of GitLab prior to 11.5.1, 11.4.8, and 11.3.11 do not send an email to the old email address when an email address change is made.  |
| Git | 2.45.2 | CVE-2018-19581 | None   | None | GitLab EE, versions 8.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure object reference vulnerability that allows a Guest user to set the weight of an issue they create.   |
| Git | 2.45.2 | CVE-2018-19582 | None   | None | GitLab EE, versions 11.4 before 11.4.8 and 11.5 before 11.5.1, is affected by an insecure direct object reference vulnerability that permits an unauthorized user to publish the draft merge request comments of another user.   |

|     |        |                      |        |      |   |
|-----|--------|----------------------|--------|------|---|
| Git | 2.45.2 | CVE-2018-19583       | MEDIUM | 6.5  | GitLab CE/EE, versions 8.0 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, would log access tokens in the Workhorse logs, permitting administrators with access to the logs to see another user's token.   |
| Git | 2.45.2 | CVE-2018-19584       | None   | None | GitLab EE, versions 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure direct object reference vulnerability that allows authenticated, but unauthorized, users to view members and milestone details of private groups.   |
| Git | 2.45.2 | CVE-2019-101031<br>4 | None   | None | Gitea 1.7.2, 1.7.3 is affected by: Cross Site Scripting (XSS). The impact is: execute JavaScript in victim's browser, when the vulnerable repo page is loaded. The component is: repository's description. The attack vector is: victim must navigate to public and affected repo page.   |
| Git | 2.45.2 | CVE-2019-13915       | None   | None | b3log Wide before 1.6.0 allows three types of attacks to access arbitrary files. First, the attacker can write code in the editor, and compile and run it approximately three times to read an arbitrary file. Second, the attacker can create a symlink, and then place the symlink into a ZIP archive. An unzip operation leads to read access, and write access (depending on file permissions), to the symlink target. Third, the attacker can import a Git repository that contains a symlink, similarly leading to read and write access. |
| Git | 2.45.2 | CVE-2019-101026<br>1 | None   | None | Gitea 1.7.0 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attacker is able to have victim execute arbitrary JS in browser. The component is: go-get URL generation - PR to fix: <a href="https://github.com/go-gitea/gitea/pull/5905">https://github.com/go-gitea/gitea/pull/5905</a> . The attack vector is: victim must open a specifically crafted URL. The fixed version is: 1.7.1 and later.  |
| Git | 2.45.2 | CVE-2018-20894       | None   | None | cPanel before 74.0.0 makes web-site contents accessible to other local users via Git repositories (SEC-443).  |
| Git | 2.45.2 | CVE-2019-10371       | HIGH   | 7.5  | A session fixation vulnerability in Jenkins Gitlab Authentication Plugin 1.4 and earlier in GitLabSecurityRealm.java allows unauthorized attackers to impersonate another user if they can control the pre-authentication session.  |
| Git | 2.45.2 | CVE-2019-10372       | MEDIUM | 6.1  | An open redirect vulnerability in Jenkins Gitlab Authentication Plugin 1.4 and earlier in GitLabSecurityRealm.java allows attackers to redirect users to a URL outside Jenkins after successful login.  |

|     |        |                |        |      |   |
|-----|--------|----------------|--------|------|---|
| Git | 2.45.2 | CVE-2019-1211  | None   | None | An elevation of privilege vulnerability exists in Git for Visual Studio when it improperly parses configuration files. An attacker who successfully exploited the vulnerability could execute code in the context of another local user. To exploit the vulnerability, an authenticated attacker would need to modify Git configuration files on a system prior to a full installation of the application. The attacker would then need to convince another user on the system to execute specific Git commands. The update addresses the issue by changing the permissions required to edit configuration files. |
| Git | 2.45.2 | CVE-2019-13139 | None   | None | In Docker before 18.09.4, an attacker who is capable of supplying or manipulating the build path for the "docker build" command would be able to gain command execution. An issue exists in the way "docker build" processes remote git URLs, and results in command injection into the underlying "git clone" command, leading to code execution in the context of the user executing the "docker build" command. This occurs because git ref can be misinterpreted as a flag.   |
| Git | 2.45.2 | CVE-2019-14943 | None   | None | An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.1.4. It uses Hard-coded Credentials.   |
| Git | 2.45.2 | CVE-2019-5461  | LOW    | 3.5  | An input validation problem was discovered in the GitHub service integration which could result in an attacker being able to make arbitrary POST requests in a GitLab instance's internal network. This vulnerability was addressed in 12.1.2, 12.0.4, and 11.11.6.   |
| Git | 2.45.2 | CVE-2019-5463  | MEDIUM | 5.3  | An authorization issue was discovered in the GitLab CE/EE CI badge images endpoint which could result in disclosure of the build status. This vulnerability was addressed in 12.1.2, 12.0.4, and 11.11.6.   |
| Git | 2.45.2 | CVE-2019-5467  | MEDIUM | 5.4  | An input validation and output encoding issue was discovered in the GitLab CE/EE wiki pages feature which could result in a persistent XSS. This vulnerability was addressed in 12.1.2, 12.0.4, and 11.11.6.  |
| Git | 2.45.2 | CVE-2019-5471  | MEDIUM | 5.4  | An input validation and output encoding issue was discovered in the GitLab email notification feature which could result in a persistent XSS. This was addressed in GitLab 12.1.2, 12.0.4, and 11.11.6.   |
| Git | 2.45.2 | CVE-2019-5473  | HIGH   | 7.2  | An authentication issue was discovered in GitLab that allowed a bypass of email verification. This was addressed in GitLab 12.1.2 and 12.0.4.   |

|     |        |                |        |     |  |
|-----|--------|----------------|--------|-----|--|
| Git | 2.45.2 | CVE-2019-11544 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 8.x, 9.x, 10.x, and 11.x before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. It allows Information Disclosure. Non-member users who subscribe to notifications of an internal project with issue and repository restrictions will receive emails about restricted events. |
| Git | 2.45.2 | CVE-2019-11545 | MEDIUM | 4.3 | An issue was discovered in GitLab Community Edition 11.9.x before 11.9.10 and 11.10.x before 11.10.2. It allows Information Disclosure. When an issue is moved to a private project, the private project namespace is leaked to unauthorized users with access to the original issue.  |
| Git | 2.45.2 | CVE-2019-11546 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. It has a Race Condition which could allow users to approve a merge request multiple times and potentially reach the approval count required to merge.   |
| Git | 2.45.2 | CVE-2019-11547 | MEDIUM | 6.1 | An issue was discovered in GitLab Community and Enterprise Edition before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. It has Improper Encoding or Escaping of Output. The branch name on new merge request notification emails isn't escaped, which could potentially lead to XSS issues.   |
| Git | 2.45.2 | CVE-2019-11548 | MEDIUM | 5.4 | An issue was discovered in GitLab Community and Enterprise Edition before 11.8.9. It has Incorrect Access Control. Unprivileged members of a project are able to post comments on confidential issues through an authorization issue in the note endpoint.   |
| Git | 2.45.2 | CVE-2019-11549 | MEDIUM | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition 9.x, 10.x, and 11.x before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. GitLab has allows an information disclosure issue where HTTP/GIT credentials are included in logs on connection errors.   |
| Git | 2.45.2 | CVE-2019-11605 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 11.8.x before 11.8.10, 11.9.x before 11.9.11, and 11.10.x before 11.10.3. It allows Information Disclosure. A small number of GitLab API endpoints would disclose project information when using a read_user scoped token.  |
| Git | 2.45.2 | CVE-2019-6782  | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 1 of 6). An authorization issue allows the contributed project information of a private profile to be viewed.  |

|     |        |               |        |     |   |
|-----|--------|---------------|--------|-----|---|
| Git | 2.45.2 | CVE-2019-6783 | HIGH   | 8.8 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. GitLab Pages contains a directory traversal vulnerability that could lead to remote command execution.  |
| Git | 2.45.2 | CVE-2019-6784 | MEDIUM | 6.1 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows XSS (issue 1 of 2). Markdown fields contain a lack of input validation and output encoding when processing KaTeX that results in a persistent XSS.  |
| Git | 2.45.2 | CVE-2019-6785 | MEDIUM | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Denial of Service. Inputting an overly long string into a Markdown field could cause a denial of service.   |
| Git | 2.45.2 | CVE-2019-6786 | MEDIUM | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control (issue 1 of 3). The contents of an LFS object can be accessed by an unauthorized user, if the file size and OID are known.  |
| Git | 2.45.2 | CVE-2019-6788 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 3 of 6). For installations using GitHub or Bitbucket OAuth integrations, it is possible to use a covert redirect to obtain the user OAuth token for those services.                             |
| Git | 2.45.2 | CVE-2019-6789 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 4 of 6). In some cases, users without project permissions will receive emails after a project move. For private projects, this will disclose the new project namespace to an unauthorized user. |
| Git | 2.45.2 | CVE-2019-6792 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Path Disclosure. When an error is encountered on project import, the error message will display instance internal information.  |
| Git | 2.45.2 | CVE-2019-6793 | HIGH   | 7.0 | An issue was discovered in GitLab Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The Jira integration feature is vulnerable to an unauthenticated blind SSRF issue.  |

|     |        |               |          |     |  |
|-----|--------|---------------|----------|-----|--|
| Git | 2.45.2 | CVE-2019-6794 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 5 of 6). A project guest user can view the last commit status of the default branch.   |
| Git | 2.45.2 | CVE-2019-6795 | MEDIUM   | 5.4 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Insufficient Visual Distinction of Homoglyphs Presented to a User. IDN homoglyphs and RTLO characters are rendered to unicode, which could be used for social engineering.          |
| Git | 2.45.2 | CVE-2019-6960 | CRITICAL | 9.8 | An issue was discovered in GitLab Community and Enterprise Edition 9.x, 10.x, and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. Access to the internal wiki is permitted when an external wiki service is enabled.  |
| Git | 2.45.2 | CVE-2019-6995 | MEDIUM   | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition 8.x, 9.x, 10.x, and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. Users are able to comment on locked project issues.  |
| Git | 2.45.2 | CVE-2019-6996 | MEDIUM   | 4.3 | An issue was discovered in GitLab Enterprise Edition 10.x (starting in 10.6) and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. The merge request approvers section has an access control issue that permits project maintainers to view membership of private groups. |
| Git | 2.45.2 | CVE-2019-6997 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting in 10.7) and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. System notes contain an access control issue that permits a guest user to view merge request titles.                     |
| Git | 2.45.2 | CVE-2019-6791 | MEDIUM   | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control (issue 3 of 3). When a project with visibility more permissive than the target group is imported, it will retain its prior visibility.                     |
| Git | 2.45.2 | CVE-2019-7176 | LOW      | 3.7 | An issue was discovered in GitLab Community and Enterprise Edition 8.x (starting in 8.9), 9.x, 10.x, and 11.x before 11.5.9, 11.6.x before 11.6.7, and 11.7.x before 11.7.2. It has Incorrect Access Control. Guest users are able to add reaction emojis on comments to which they have no visibility.                      |

|     |        |                |          |      |  |
|-----|--------|----------------|----------|------|--|
| Git | 2.45.2 | CVE-2019-10392 | HIGH     | 8.8  | Jenkins Git Client Plugin 2.8.4 and earlier and 3.0.0-rc did not properly restrict values passed as URL argument to an invocation of 'git ls-remote', resulting in OS command injection.   |
| Git | 2.45.2 | CVE-2019-5485  | CRITICAL | 10.0 | NPM package gitlabhook version 0.0.17 is vulnerable to a Command Injection vulnerability. Arbitrary commands can be injected through the repository name.  |
| Git | 2.45.2 | CVE-2019-16170 | HIGH     | 7.1  | An issue was discovered in GitLab Enterprise Edition 11.x and 12.x before 12.0.9, 12.1.x before 12.1.9, and 12.2.x before 12.2.5. It has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2019-15721 | MEDIUM   | 5.4  | An issue was discovered in GitLab Community and Enterprise Edition 10.8 through 12.2.1. An internal endpoint unintentionally allowed group maintainers to view and edit group runner settings.   |
| Git | 2.45.2 | CVE-2019-15722 | HIGH     | 7.5  | An issue was discovered in GitLab Community and Enterprise Edition 8.15 through 12.2.1. Particular mathematical expressions in GitLab Markdown can exhaust client resources.   |
| Git | 2.45.2 | CVE-2019-15723 | MEDIUM   | 5.3  | An issue was discovered in GitLab Community and Enterprise Edition 11.9.x and 11.10.x before 11.10.1. Merge requests created by email could be used to bypass push rules in certain situations.  |
| Git | 2.45.2 | CVE-2019-15724 | MEDIUM   | 6.1  | An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.2.1. Label descriptions are vulnerable to HTML injection.  |
| Git | 2.45.2 | CVE-2019-15725 | HIGH     | 7.5  | An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.2.1. An IDOR in the epic notes API that could result in disclosure of private milestones, labels, and other information.  |
| Git | 2.45.2 | CVE-2019-15726 | MEDIUM   | 5.3  | An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Embedded images and media files in markdown could be pointed to an arbitrary server, which would reveal the IP address of clients requesting the file from that server. |
| Git | 2.45.2 | CVE-2019-15727 | MEDIUM   | 5.3  | An issue was discovered in GitLab Community and Enterprise Edition 11.2 through 12.2.1. Insufficient permission checks were being applied when displaying CI results, potentially exposing some CI metrics data to unauthorized users.                     |

|     |        |                |        |     |  |
|-----|--------|----------------|--------|-----|--|
| Git | 2.45.2 | CVE-2019-15728 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 10.1 through 12.2.1. Protections against SSRF attacks on the Kubernetes integration are insufficient, which could have allowed an attacker to request any local network resource accessible from the GitLab server.   |
| Git | 2.45.2 | CVE-2019-15730 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 8.14 through 12.2.1. The Jira integration contains a SSRF vulnerability as a result of a bypass of the current protection mechanisms against this type of attack, which would allow sending requests to any resources accessible in the local network by the GitLab server. |
| Git | 2.45.2 | CVE-2019-15731 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.2.1. Non-members were able to comment on merge requests despite the repository being set to allow only project members to do so.  |
| Git | 2.45.2 | CVE-2019-15732 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 12.2 through 12.2.1. The project import API could be used to bypass project visibility restrictions.  |
| Git | 2.45.2 | CVE-2019-15733 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 7.12 through 12.2.1. The specified default branch name could be exposed to unauthorized users.  |
| Git | 2.45.2 | CVE-2019-15734 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 8.6 through 12.2.1. Under very specific conditions, commit titles and team member comments could become viewable to users who did not have permission to access these.  |
| Git | 2.45.2 | CVE-2019-15736 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Under certain circumstances, CI pipelines could potentially be used in a denial of service attack.  |
| Git | 2.45.2 | CVE-2019-15737 | MEDIUM | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Certain account actions needed improved authentication and session management.  |
| Git | 2.45.2 | CVE-2019-15738 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.2.1. Under certain conditions, merge request IDs were being disclosed via email.  |
| Git | 2.45.2 | CVE-2019-15739 | MEDIUM | 6.1 | An issue was discovered in GitLab Community and Enterprise Edition 8.1 through 12.2.1. Certain areas displaying Markdown were not properly sanitizing some XSS payloads.   |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2019-15740 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 7.9 through 12.2.1. EXIF Geolocation data was not being removed from certain image uploads.  |
| Git | 2.45.2 | CVE-2019-15741 | CRITICAL | 9.8 | An issue was discovered in GitLab Omnibus 7.4 through 12.2.1. An unsafe interaction with logrotate could result in a privilege escalation   |
| Git | 2.45.2 | CVE-2019-15729 | HIGH     | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 8.18 through 12.2.1. An internal endpoint unintentionally disclosed information about the last pipeline that ran for a merge request.  |
| Git | 2.45.2 | CVE-2019-15000 | CRITICAL | 9.8 | The commit diff rest endpoint in Bitbucket Server and Data Center before 5.16.10 (the fixed version for 5.16.x ), from 6.0.0 before 6.0.10 (the fixed version for 6.0.x), from 6.1.0 before 6.1.8 (the fixed version for 6.1.x), from 6.2.0 before 6.2.6 (the fixed version for 6.2.x), from 6.3.0 before 6.3.5 (the fixed version for 6.3.x), from 6.4.0 before 6.4.3 (the fixed version for 6.4.x), and from 6.5.0 before 6.5.2 (the fixed version for 6.5.x) allows remote attackers who have permission to access a repository, if public access is enabled for a project or repository then attackers are able to exploit this issue anonymously, to read the contents of arbitrary files on the system and execute commands via injecting additional arguments into git commands. |
| Git | 2.45.2 | CVE-2019-10414 | MEDIUM   | 6.5 | Jenkins Git Changelog Plugin 2.17 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.  |
| Git | 2.45.2 | CVE-2019-10415 | MEDIUM   | 6.5 | Jenkins Violation Comments to GitLab Plugin 2.28 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system.   |
| Git | 2.45.2 | CVE-2019-10416 | MEDIUM   | 6.5 | Jenkins Violation Comments to GitLab Plugin 2.28 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.   |
| Git | 2.45.2 | CVE-2019-10429 | MEDIUM   | 5.5 | Jenkins GitLab Logo Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.   |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2019-14957 | MEDIUM   | 5.3 | The JetBrains Vim plugin before version 0.52 was storing individual project data in the global vim_settings.xml file. This xml file could be synchronized to a publicly accessible GitHub repository.   |
| Git | 2.45.2 | CVE-2019-17263 | LOW      | 3.3 | In libyal libfws before 20191006, libfws_extension_block_copy_from_byte_stream in libfws_extension_block.c has a heap-based buffer over-read because rejection of an unsupported size only considers values less than 6, even though values of 6 and 7 are also unsupported. NOTE: the vendor has disputed this as described in the GitHub issue                                      |
| Git | 2.45.2 | CVE-2019-17264 | LOW      | 3.3 | In libyal liblnk before 20191006, liblnk_location_information_read_data in liblnk_location_information.c has a heap-based buffer over-read because an incorrect variable name is used for a certain offset. NOTE: the vendor has disputed this as described in the GitHub issue   |
| Git | 2.45.2 | CVE-2019-17401 | LOW      | 3.3 | libyal liblnk 20191006 has a heap-based buffer over-read in the network_share_name_offset>20 code block of liblnk_location_information_read_data in liblnk_location_information.c, a different issue than CVE-2019-17264. NOTE: the vendor has disputed this as described in the GitHub issue   |
| Git | 2.45.2 | CVE-2010-2447  | CRITICAL | 9.8 | gitolite before 1.4.1 does not filter src/ or hooks/ from path names.   |
| Git | 2.45.2 | CVE-2019-19022 | HIGH     | 7.5 | iTerm2 through 3.3.6 has potentially insufficient documentation about the presence of search history in com.googlecode.iterm2.plist, which might allow remote attackers to obtain sensitive information, as demonstrated by searching for the NoSyncSearchHistory string in .plist files within public Git repositories.  |
| Git | 2.45.2 | CVE-2019-18933 | CRITICAL | 9.8 | In Zulip Server versions from 1.7.0 to before 2.0.7, a bug in the new user signup process meant that users who registered their account using social authentication (e.g., GitHub or Google SSO) in an organization that also allows password authentication could have their personal API key stolen by an unprivileged attacker, allowing nearly full access to the user's account. |
| Git | 2.45.2 | CVE-2019-15593 | MEDIUM   | 6.5 | GitLab 12.2.3 contains a security vulnerability that allows a user to affect the availability of the service through a Denial of Service attack in Issue Comments.  |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2019-18460 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 8.15 through 12.4 in the Comments Search feature provided by the Elasticsearch integration. It has Incorrect Access Control. |
| Git | 2.45.2 | CVE-2019-18461 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.3 through 12.3 when a sub group epic is added to a public group. It has Incorrect Access Control.                         |
| Git | 2.45.2 | CVE-2019-18462 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.3 through 12.4. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-18463 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition through 12.4. It has Insecure Permissions (issue 4 of 4).  |
| Git | 2.45.2 | CVE-2019-18457 | HIGH   | 8.8 | An issue was discovered in GitLab Community and Enterprise Edition 11.8 through 12.4 when handling Security tokens.. It has Insecure Permissions.   |
| Git | 2.45.2 | CVE-2019-18458 | LOW    | 2.7 | An issue was discovered in GitLab Community and Enterprise Edition through 12.4. It has Insecure Permissions (issue 2 of 4).  |
| Git | 2.45.2 | CVE-2019-18459 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.3 to 12.3 in the protected environments feature. It has Insecure Permissions (issue 3 of 4).                              |
| Git | 2.45.2 | CVE-2019-18446 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 8.15 through 12.4. It has Insecure Permissions (issue 1 of 2).   |
| Git | 2.45.2 | CVE-2019-18447 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 12.4. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-18448 | MEDIUM | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition before 12.4. It has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-18449 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 12.4 in the autocomplete feature. It has Insecure Permissions (issue 2 of 2).   |
| Git | 2.45.2 | CVE-2019-18450 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 12.4 in the Project labels feature. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-18451 | MEDIUM | 6.1 | An issue was discovered in GitLab Community and Enterprise Edition 10.7.4 through 12.4 in the InternalRedirect filtering feature. It has an Open Redirect.                                      |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2019-18452 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.3 through 12.4 when moving an issue to a public project from a private one. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-18453 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.6 through 12.4 in the add comments via email feature. It has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-18454 | MEDIUM   | 6.1 | An issue was discovered in GitLab Community and Enterprise Edition 10.5 through 12.4 in link validation for RDoc wiki pages feature. It has XSS.  |
| Git | 2.45.2 | CVE-2019-18455 | HIGH     | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 11 through 12.4 when building Nested GraphQL queries. It has a large or infinite loop.   |
| Git | 2.45.2 | CVE-2019-18456 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 8.17 through 12.4 in the Search feature provided by Elasticsearch integration.. It has Insecure Permissions (issue 1 of 4).  |
| Git | 2.45.2 | CVE-2019-19596 | MEDIUM   | 5.4 | GitBook through 2.6.9 allows XSS via a local .md file.  |
| Git | 2.45.2 | CVE-2019-19617 | CRITICAL | 9.8 | phpMyAdmin before 4.9.2 does not escape certain Git information, related to libraries/classes/Display/GitRevision.php and libraries/classes/Footer.php.   |
| Git | 2.45.2 | CVE-2019-19604 | HIGH     | 7.8 | Arbitrary command execution is possible in Git before 2.20.2, 2.21.x before 2.21.1, 2.22.x before 2.22.2, 2.23.x before 2.23.1, and 2.24.x before 2.24.1 because a "git submodule update" operation can run commands found in the .gitmodules file of a malicious repository. |
| Git | 2.45.2 | CVE-2019-15575 | HIGH     | 7.5 | A command injection exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to inject commands via the API through the blobs scope.   |
| Git | 2.45.2 | CVE-2019-15576 | HIGH     | 7.5 | An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to view private system notes from a GraphQL endpoint.   |
| Git | 2.45.2 | CVE-2019-15577 | MEDIUM   | 4.3 | An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed project milestones to be disclosed via groups browsing.   |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2019-15580 | MEDIUM | 6.5 | An information exposure vulnerability exists in gitlab.com <v12.3.2, <v12.2.6, and <v12.1.10 when using the blocking merge request feature, it was possible for an unauthenticated user to see the head pipeline data of a public project even though pipeline visibility was restricted.   |
| Git | 2.45.2 | CVE-2019-15589 | HIGH   | 8.8 | An improper access control vulnerability exists in Gitlab <v12.3.2, <v12.2.6, <v12.1.12 which would allow a blocked user would be able to use GIT clone and pull if he had obtained a CI/CD token before.   |
| Git | 2.45.2 | CVE-2019-15591 | MEDIUM | 6.5 | An improper access control vulnerability exists in GitLab <12.3.3 that allows an attacker to obtain container and dependency scanning reports through the merge request widget even though public pipelines were disabled.  |
| Git | 2.45.2 | CVE-2019-1387  | HIGH   | 8.8 | An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones. |
| Git | 2.45.2 | CVE-2019-5469  | MEDIUM | 6.5 | An IDOR vulnerability exists in GitLab <v12.1.2, <v12.0.4, and <v11.11.6 that allowed uploading files from project archive to replace other users files potentially allowing an attacker to replace project binaries or other uploaded assets.  |
| Git | 2.45.2 | CVE-2019-5486  | HIGH   | 8.8 | A authentication bypass vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 in the Salesforce login integration that could be used by an attacker to create an account that bypassed domain restrictions and email verification requirements.  |
| Git | 2.45.2 | CVE-2019-5487  | MEDIUM | 5.3 | An improper access control vulnerability exists in Gitlab EE <v12.3.3, <v12.2.7, & <v12.1.13 that allowed the group search feature with Elasticsearch to return private code, merge requests and commits.   |
| Git | 2.45.2 | CVE-2019-15584 | MEDIUM | 6.5 | A denial of service exists in gitlab <v12.3.2, <v12.2.6, and <v12.1.10 that would let an attacker bypass input validation in markdown fields take down the affected page.   |
| Git | 2.45.2 | CVE-2018-20492 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control (issue 2 of 6).  |

|     |        |                |        |     |  |
|-----|--------|----------------|--------|-----|--|
| Git | 2.45.2 | CVE-2018-20488 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows Information Exposure.                   |
| Git | 2.45.2 | CVE-2018-20489 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.                  |
| Git | 2.45.2 | CVE-2018-20490 | MEDIUM | 5.4 | An issue was discovered in GitLab Community and Enterprise Edition 11.2.x through 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.              |
| Git | 2.45.2 | CVE-2018-20491 | MEDIUM | 5.4 | An issue was discovered in GitLab Enterprise Edition 11.3.x and 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.                                |
| Git | 2.45.2 | CVE-2018-20493 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.                  |
| Git | 2.45.2 | CVE-2018-20494 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.                  |
| Git | 2.45.2 | CVE-2018-20495 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.3.x and 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows Information Exposure. |
| Git | 2.45.2 | CVE-2018-20496 | MEDIUM | 5.4 | An issue was discovered in GitLab Community and Enterprise Edition 11.2.x through 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.              |
| Git | 2.45.2 | CVE-2018-20497 | MEDIUM | 5.0 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows SSRF.                                   |
| Git | 2.45.2 | CVE-2018-20498 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.                  |
| Git | 2.45.2 | CVE-2018-20499 | HIGH   | 7.2 | An issue was discovered in GitLab Community and Enterprise Edition before 11.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows SSRF.                       |
| Git | 2.45.2 | CVE-2018-20501 | MEDIUM | 6.3 | An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.                  |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2018-20507 | MEDIUM   | 5.3 | An issue was discovered in GitLab Enterprise Edition 11.2.x through 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control. |
| Git | 2.45.2 | CVE-2019-19086 | MEDIUM   | 4.3 | Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 1 of 2).   |
| Git | 2.45.2 | CVE-2019-19087 | MEDIUM   | 4.3 | Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 2 of 2).   |
| Git | 2.45.2 | CVE-2019-19088 | CRITICAL | 9.8 | Gitlab Enterprise Edition (EE) 11.3 through 12.4.2 allows Directory Traversal.  |
| Git | 2.45.2 | CVE-2019-19254 | MEDIUM   | 5.3 | GitLab Community Edition (CE) and Enterprise Edition (EE). 9.6 and later through 12.5 has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2019-19311 | MEDIUM   | 5.4 | GitLab EE 8.14 through 12.5, 12.4.3, and 12.3.6 allows XSS in group and profile fields.   |
| Git | 2.45.2 | CVE-2019-19255 | MEDIUM   | 4.3 | GitLab Enterprise Edition (EE) 12.3 and later through 12.5 has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-19256 | MEDIUM   | 5.3 | GitLab Enterprise Edition (EE) 12.2 and later through 12.5 has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-19257 | MEDIUM   | 5.3 | GitLab Community Edition (CE) and Enterprise Edition (EE) through 12.5 has Incorrect Access Control (issue 1 of 2).   |
| Git | 2.45.2 | CVE-2019-19258 | MEDIUM   | 5.3 | GitLab Enterprise Edition (EE) 10.8 and later through 12.5 has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-19259 | MEDIUM   | 4.3 | GitLab Enterprise Edition (EE) 11.3 and later through 12.5 allows an Insecure Direct Object Reference (IDOR).   |
| Git | 2.45.2 | CVE-2019-19260 | MEDIUM   | 5.4 | GitLab Community Edition (CE) and Enterprise Edition (EE) through 12.5 has Incorrect Access Control (issue 2 of 2).   |
| Git | 2.45.2 | CVE-2019-19261 | HIGH     | 8.8 | GitLab Enterprise Edition (EE) 6.7 and later through 12.5 allows SSRF.  |
| Git | 2.45.2 | CVE-2019-19262 | MEDIUM   | 4.3 | GitLab Enterprise Edition (EE) 11.9 and later through 12.5 has Insecure Permissions.  |
| Git | 2.45.2 | CVE-2019-19263 | MEDIUM   | 4.3 | GitLab Enterprise Edition (EE) 8.2 and later through 12.5 has Insecure Permissions.   |
| Git | 2.45.2 | CVE-2019-19309 | MEDIUM   | 4.3 | GitLab Enterprise Edition (EE) 8.90 and later through 12.5 has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-19310 | MEDIUM   | 4.9 | GitLab Enterprise Edition (EE) 9.0 and later through 12.5 allows Information Disclosure.  |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2019-19312 | MEDIUM   | 5.8 | GitLab EE 8.14 through 12.5, 12.4.3, and 12.3.6 has Incorrect Access Control. After a project changed to private, previously forked repositories were still able to get information about the private project through the API.  |
| Git | 2.45.2 | CVE-2019-19313 | HIGH     | 7.5 | GitLab EE 12.3 through 12.5, 12.4.3, and 12.3.6 allows Denial of Service. Certain characters were making it impossible to create, edit, or view issues and commits.   |
| Git | 2.45.2 | CVE-2019-19314 | HIGH     | 7.5 | GitLab EE 8.4 through 12.5, 12.4.3, and 12.3.6 stored several tokens in plaintext.  |
| Git | 2.45.2 | CVE-2019-19628 | CRITICAL | 9.8 | In GitLab EE 11.3 through 12.5.3, 12.4.5, and 12.3.8, insufficient parameter sanitization for the Maven package registry could lead to privilege escalation and remote code execution vulnerabilities under certain conditions. |
| Git | 2.45.2 | CVE-2019-19629 | HIGH     | 7.5 | In GitLab EE 10.5 through 12.5.3, 12.4.5, and 12.3.8, when transferring a public project to a private group, private code would be disclosed via the Group Search API provided by the Elasticsearch integration.                |
| Git | 2.45.2 | CVE-2019-10776 | CRITICAL | 9.8 | In "index.js" file line 240, the run command executes the git command with a user controlled variable called remoteUrl. This affects git-diff-apply all versions prior to 0.22.2.   |
| Git | 2.45.2 | CVE-2019-20145 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 11.4 through 12.6.1. It has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-20146 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 11.0 through 12.6. It allows Uncontrolled Resource Consumption.  |
| Git | 2.45.2 | CVE-2019-20147 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 9.1 through 12.6.1. It has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2019-20148 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 8.13 through 12.6.1. It has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2020-5197  | MEDIUM   | 4.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 5.1 through 12.6.1. It has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2020-6832  | MEDIUM   | 5.3 | An issue was discovered in GitLab Enterprise Edition (EE) 8.9.0 through 12.6.1. Using the project import feature, it was possible for someone to obtain issues from private projects.   |

|     |        |                |        |     |  |
|-----|--------|----------------|--------|-----|--|
| Git | 2.45.2 | CVE-2019-20142 | MEDIUM | 4.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 12.3 through 12.6.1. It allows Denial of Service.   |
| Git | 2.45.2 | CVE-2019-20143 | MEDIUM | 5.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 12.6. It has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-20144 | MEDIUM | 4.3 | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) 10.8 through 12.6.1. It has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2020-2096  | MEDIUM | 6.1 | Jenkins Gitlab Hook Plugin 1.4.2 and earlier does not escape project names in the build_now endpoint, resulting in a reflected XSS vulnerability.  |
| Git | 2.45.2 | CVE-2019-1349  | HIGH   | 8.8 | A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1350, CVE-2019-1352, CVE-2019-1354, CVE-2019-1387.  |
| Git | 2.45.2 | CVE-2019-1350  | HIGH   | 8.8 | A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1349, CVE-2019-1352, CVE-2019-1354, CVE-2019-1387.  |
| Git | 2.45.2 | CVE-2019-1351  | HIGH   | 7.5 | A tampering vulnerability exists when Git for Visual Studio improperly handles virtual drive paths, aka 'Git for Visual Studio Tampering Vulnerability'.   |
| Git | 2.45.2 | CVE-2019-1352  | HIGH   | 8.8 | A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1349, CVE-2019-1350, CVE-2019-1354, CVE-2019-1387.  |
| Git | 2.45.2 | CVE-2019-1354  | HIGH   | 8.8 | A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1349, CVE-2019-1350, CVE-2019-1352, CVE-2019-1387.  |
| Git | 2.45.2 | CVE-2019-1348  | LOW    | 3.3 | An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. The --export-marks option of git fast-import is exposed also via the in-stream command feature export-marks=... and it allows overwriting arbitrary paths. |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2019-1353  | CRITICAL | 9.8 | An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. When running Git in the Windows Subsystem for Linux (also known as "WSL") while accessing a working directory on a regular Windows drive, none of the NTFS protections were active. |
| Git | 2.45.2 | CVE-2019-15578 | MEDIUM   | 5.3 | An information disclosure exists in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE). The path of a private project, that used to be public, would be disclosed in the unsubscribe email link of issues and merge requests.  |
| Git | 2.45.2 | CVE-2019-15579 | MEDIUM   | 5.3 | An information disclosure exists in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE) where the assignee(s) of a confidential issue in a private project would be disclosed to a guest via milestones.  |
| Git | 2.45.2 | CVE-2019-15581 | MEDIUM   | 5.3 | An IDOR exists in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE) that allowed a project owner or maintainer to see the members of any private group via merge request approval rules.  |
| Git | 2.45.2 | CVE-2019-15582 | MEDIUM   | 5.3 | An IDOR was discovered in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE) that allowed a maintainer to add any private group to a protected environment.  |
| Git | 2.45.2 | CVE-2019-15583 | HIGH     | 7.5 | An information disclosure exists in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE). When an issue was moved to a public project from a private one, the associated private labels and the private project namespace would be disclosed through the GitLab API.             |
| Git | 2.45.2 | CVE-2019-15585 | CRITICAL | 9.8 | Improper authentication exists in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE) in the GitLab SAML integration had a validation issue that permitted an attacker to takeover another user's account.  |
| Git | 2.45.2 | CVE-2019-15586 | MEDIUM   | 6.1 | A XSS exists in Gitlab CE/EE < 12.1.10 in the Mermaid plugin.   |
| Git | 2.45.2 | CVE-2019-15590 | HIGH     | 7.5 | An access control issue exists in < 12.3.5, < 12.2.8, and < 12.1.14 for GitLab Community Edition (CE) and Enterprise Edition (EE) where private merge requests and issues would be disclosed with the Group Search feature provided by Elasticsearch integration  |

|     |        |               |          |     |   |
|-----|--------|---------------|----------|-----|---|
| Git | 2.45.2 | CVE-2019-5462 | HIGH     | 8.8 | A privilege escalation issue was discovered in GitLab CE/EE 9.0 and later when trigger tokens are not rotated once ownership of them has changed.   |
| Git | 2.45.2 | CVE-2019-5464 | CRITICAL | 9.8 | A flawed DNS rebinding protection issue was discovered in GitLab CE/EE 10.2 and later in the <code>`url_blocker.rb`</code> which could result in SSRF where the library is utilized.  |
| Git | 2.45.2 | CVE-2019-5465 | MEDIUM   | 4.3 | An information disclosure issue was discovered in GitLab CE/EE 8.14 and later, by using the move issue feature which could result in disclosure of the newly created issue ID.  |
| Git | 2.45.2 | CVE-2019-5466 | MEDIUM   | 4.3 | An IDOR was discovered in GitLab CE/EE 11.5 and later that allowed new merge requests endpoint to disclose label names.   |
| Git | 2.45.2 | CVE-2019-5468 | HIGH     | 8.8 | An privilege escalation issue was discovered in Gitlab versions < 12.1.2, < 12.0.4, and < 11.11.6 when Mattermost slash commands are used with a blocked account.   |
| Git | 2.45.2 | CVE-2019-5470 | HIGH     | 7.5 | An information disclosure issue was discovered GitLab versions < 12.1.2, < 12.0.4, and < 11.11.6 in the security dashboard which could result in disclosure of vulnerability feedback information.  |
| Git | 2.45.2 | CVE-2019-5472 | HIGH     | 7.5 | An authorization issue was discovered in Gitlab versions < 12.1.2, < 12.0.4, and < 11.11.6 that prevented owners and maintainer to delete epic comments.  |
| Git | 2.45.2 | CVE-2019-5474 | MEDIUM   | 6.5 | An authorization issue was discovered in GitLab EE < 12.1.2, < 12.0.4, and < 11.11.6 allowing the merge request approval rules to be overridden without appropriate permissions.  |
| Git | 2.45.2 | CVE-2012-6114 | MEDIUM   | 5.5 | The <code>git-changelog</code> utility in <code>git-extras</code> 1.7.0 allows local users to overwrite arbitrary files via a symlink attack on (1) <code>/tmp/changelog</code> or (2) <code>/tmp/git-effort</code> .   |
| Git | 2.45.2 | CVE-2013-4582 | MEDIUM   | 6.5 | The (1) <code>create_branch</code> , (2) <code>create_tag</code> , (3) <code>import_project</code> , and (4) <code>fork_project</code> functions in <code>lib/gitlab_projects.rb</code> in GitLab 5.0 before 5.4.2, Community Edition before 6.2.4, Enterprise Edition before 6.2.1 and <code>gitlab-shell</code> before 1.7.8 allows remote authenticated users to include information from local files into the metadata of a Git repository via the web interface. |
| Git | 2.45.2 | CVE-2013-4583 | HIGH     | 8.8 | The <code>parse_cmd</code> function in <code>lib/gitlab_shell.rb</code> in GitLab 5.0 before 5.4.2, Community Edition before 6.2.4, and Enterprise Edition before 6.2.1 and <code>gitlab-shell</code> before 1.7.8 allows remote authenticated users to gain privileges and clone arbitrary repositories.   |

|     |        |               |                      |            |  |
|-----|--------|---------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-5234 | ['MEDIUM', 'MEDIUM'] | [4.8, 6.5] | MessagePack for C# and Unity before version 1.9.11 and 2.1.90 has a vulnerability where untrusted data can lead to DoS attack due to hash collisions and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.                                  |
| Git | 2.45.2 | CVE-2020-7979 | MEDIUM               | 5.3        | GitLab EE 8.9 and later through 12.7.2 has Insecure Permission   |
| Git | 2.45.2 | CVE-2020-8114 | CRITICAL             | 9.8        | GitLab EE 8.9 and later through 12.7.2 has Insecure Permission   |
| Git | 2.45.2 | CVE-2020-7966 | HIGH                 | 7.5        | GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.   |
| Git | 2.45.2 | CVE-2020-7967 | MEDIUM               | 4.3        | GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).  |
| Git | 2.45.2 | CVE-2020-7968 | HIGH                 | 7.5        | GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2020-7969 | HIGH                 | 7.5        | GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.  |
| Git | 2.45.2 | CVE-2020-7971 | MEDIUM               | 6.1        | GitLab EE 11.0 and later through 12.7.2 allows XSS.  |
| Git | 2.45.2 | CVE-2020-7972 | HIGH                 | 7.5        | GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).  |
| Git | 2.45.2 | CVE-2020-7973 | MEDIUM               | 6.1        | GitLab through 12.7.2 allows XSS.  |
| Git | 2.45.2 | CVE-2020-7974 | MEDIUM               | 5.3        | GitLab EE 10.1 through 12.7.2 allows Information Disclosure.   |
| Git | 2.45.2 | CVE-2020-7976 | MEDIUM               | 5.3        | GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2020-7977 | MEDIUM               | 5.3        | GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.   |
| Git | 2.45.2 | CVE-2020-7978 | HIGH                 | 7.5        | GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.  |
| Git | 2.45.2 | CVE-2020-6833 | HIGH                 | 7.5        | An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.  |
| Git | 2.45.2 | CVE-2020-8788 | MEDIUM               | 6.1        | Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report. |

|     |        |               |          |     |  |
|-----|--------|---------------|----------|-----|--|
| Git | 2.45.2 | CVE-2014-9390 | CRITICAL | 9.8 | Git before 1.8.5.6, 1.9.x before 1.9.5, 2.0.x before 2.0.5, 2.1.x before 2.1.4, and 2.2.x before 2.2.1 on Windows and OS X; Mercurial before 3.2.3 on Windows and OS X; Apple Xcode before 6.2 beta 3; mine all versions before 08-12-2014; libgit2 all versions up to 0.21.2; Egit all versions before 08-12-2014; and JGit all versions before 08-12-2014 allow remote Git servers to execute arbitrary commands via a tree containing a crafted .git/config file with (1) an ignorable Unicode codepoint, (2) a git-1/config representation, or (3) mixed case that is improperly handled on a case-insensitive filesystem. |
| Git | 2.45.2 | CVE-2020-2112 | MEDIUM   | 5.4 | Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the parameter name shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.   |
| Git | 2.45.2 | CVE-2020-2113 | MEDIUM   | 5.4 | Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the default value shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.  |
| Git | 2.45.2 | CVE-2020-2116 | HIGH     | 8.8 | A cross-site request forgery vulnerability in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.   |
| Git | 2.45.2 | CVE-2020-2117 | MEDIUM   | 4.3 | A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.  |
| Git | 2.45.2 | CVE-2020-2118 | MEDIUM   | 4.3 | A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.  |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2020-5239  | ['HIGH', 'HIGH'] | [8.7, 8.8] | In Mailu before version 1.7, an authenticated user can exploit a vulnerability in Mailu fetchmail script and gain full access to a Mailu instance. Mailu servers that have open registration or untrusted users are most impacted. The master and 1.7 branches are patched on our git repository. All Docker images published on docker.io/mailu for tags 1.5, 1.6, 1.7 and master are patched. For detailed instructions about patching and securing the server afterwards, see <a href="https://github.com/Mailu/Mailu/issues/1354">https://github.com/Mailu/Mailu/issues/1354</a> |
| Git | 2.45.2 | CVE-2019-15592 | MEDIUM           | 4.3        | GitLab 12.2.2 and below contains a security vulnerability that allows a guest user in a private project to see the merge request ID associated to an issue via the activity timeline.  |
| Git | 2.45.2 | CVE-2019-15594 | MEDIUM           | 4.3        | GitLab 11.8 and later contains a security vulnerability that allows a user to obtain details of restricted pipelines via the merge request endpoint.   |
| Git | 2.45.2 | CVE-2019-12825 | MEDIUM           | 4.3        | Unauthorized Access to the Container Registry of other groups was discovered in GitLab Enterprise 12.0.0-pre. In other words, authenticated remote attackers can read Docker registries of other groups. When a legitimate user changes the path of a group, Docker registries are not adapted, leaving them in the old namespace. They are not protected and are available to all other users with no previous access to the repo.  |
| Git | 2.45.2 | CVE-2020-8795  | HIGH             | 7.5        | In GitLab Enterprise Edition (EE) 12.5.0 through 12.7.5, sharing a group with a group could grant project access to unauthorized users.  |
| Git | 2.45.2 | CVE-2019-10802 | CRITICAL         | 9.8        | giting version prior to 0.0.8 allows execution of arbitrary commands. The first argument "repo" of function "pull()" is executed by the package without any validation.  |
| Git | 2.45.2 | CVE-2020-8113  | CRITICAL         | 9.8        | GitLab 10.7 and later through 12.7.2 has Incorrect Access Control.   |
| Git | 2.45.2 | CVE-2020-2136  | MEDIUM           | 5.4        | Jenkins Git Plugin 4.2.0 and earlier does not escape the error message for the repository URL for Microsoft TFS field form validation, resulting in a stored cross-site scripting vulnerability.   |
| Git | 2.45.2 | CVE-2019-12428 | CRITICAL         | 9.8        | An issue was discovered in GitLab Community and Enterprise Edition 6.8 through 11.11. Users could bypass the mandatory external authentication provider sign-in restrictions by sending a specially crafted request. It has Improper Authorization.  |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2019-12429 | MEDIUM   | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition 11.9 through 11.11. Unprivileged users were able to access labels, status and merge request counts of confidential issues via the milestone details page. It has Improper Access Control.   |
| Git | 2.45.2 | CVE-2019-12430 | HIGH     | 8.8 | An issue was discovered in GitLab Community and Enterprise Edition 11.11. A specially crafted payload would allow an authenticated malicious user to execute commands remotely through the repository download feature. It allows Command Injection.           |
| Git | 2.45.2 | CVE-2019-12431 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 8.13 through 11.11. Restricted users could access the metadata of private milestones through the Search API. It has Improper Access Control.  |
| Git | 2.45.2 | CVE-2019-12432 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 8.13 through 11.11. Non-member users who subscribed to issue notifications could access the title of confidential issues through the unsubscription page. It allows Information Disclosure. |
| Git | 2.45.2 | CVE-2019-12433 | MEDIUM   | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.7 through 11.11. It has Improper Input Validation. Restricted visibility settings allow creating internal projects in private groups, leading to multiple permission issues.             |
| Git | 2.45.2 | CVE-2019-12434 | MEDIUM   | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 10.6 through 11.11. Users could guess the URL slug of private projects through the contrast of the destination URLs of issues linked in comments. It allows Information Disclosure.         |
| Git | 2.45.2 | CVE-2019-12441 | HIGH     | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 8.4 through 11.11. The protected branches feature contained a access control issue which resulted in a bypass of the protected branches restriction rules. It has Incorrect Access Control. |
| Git | 2.45.2 | CVE-2019-12442 | MEDIUM   | 6.1 | An issue was discovered in GitLab Enterprise Edition 11.7 through 11.11. The epic details page contained a lack of input validation and output encoding issue which resulted in a persistent XSS vulnerability on child epics.                                 |
| Git | 2.45.2 | CVE-2019-12443 | CRITICAL | 9.8 | An issue was discovered in GitLab Community and Enterprise Edition 10.2 through 11.11. Multiple features contained Server-Side Request Forgery (SSRF) vulnerabilities caused by an insufficient validation to prevent DNS rebinding attacks.                   |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2019-12444 | MEDIUM | 6.1 | An issue was discovered in GitLab Community and Enterprise Edition 8.9 through 11.11. Wiki Pages contained a lack of input validation which resulted in a persistent XSS vulnerability.   |
| Git | 2.45.2 | CVE-2019-12445 | MEDIUM | 5.4 | An issue was discovered in GitLab Community and Enterprise Edition 8.4 through 11.11. A malicious user could execute JavaScript code on notes by importing a specially crafted project file. It allows XSS.   |
| Git | 2.45.2 | CVE-2019-12446 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition 8.3 through 11.11. It allows Information Exposure through an Error Message.  |
| Git | 2.45.2 | CVE-2019-13001 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.9 and later through 12.0.2. GitLab Snippets were vulnerable to an authorization issue that allowed unauthorized users to add comments to a private snippet. It allows authentication bypass.                                |
| Git | 2.45.2 | CVE-2019-13002 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.0.2. Unauthorized users were able to read pipeline information of the last merge request. It has Incorrect Access Control.  |
| Git | 2.45.2 | CVE-2019-13003 | HIGH   | 7.5 | An issue was discovered in GitLab Community and Enterprise Edition before 12.0.3. One of the parsers used by GitLab CI was vulnerable to a resource exhaustion attack. It allows Uncontrolled Resource Consumption.   |
| Git | 2.45.2 | CVE-2019-13004 | MEDIUM | 5.3 | An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.0.2. When specific encoded characters were added to comments, the comments section would become inaccessible. It has Incorrect Access Control (issue 1 of 2).   |
| Git | 2.45.2 | CVE-2019-13005 | MEDIUM | 4.3 | An issue was discovered in GitLab Enterprise Edition and Community Edition 1.10 through 12.0.2. The GitLab graphql service was vulnerable to multiple authorization issues that disclosed restricted user, group, and repository metadata to unauthorized users. It has Incorrect Access Control. |
| Git | 2.45.2 | CVE-2019-13006 | MEDIUM | 4.3 | An issue was discovered in GitLab Community and Enterprise Edition 9.0 and through 12.0.2. Users with access to issues, but not the repository were able to view the number of related merge requests on an issue. It has Incorrect Access Control.   |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2019-13007 | MEDIUM | 4.9 | An issue was discovered in GitLab Community and Enterprise Edition 11.11 through 12.0.2. When an admin enabled one of the service templates, it was triggering an action that leads to resource depletion. It allows Uncontrolled Resource Consumption.     |
| Git | 2.45.2 | CVE-2019-13009 | MEDIUM | 6.5 | An issue was discovered in GitLab Community and Enterprise Edition 9.2 through 12.0.2. Uploaded files associated with unsaved personal snippets were accessible to unauthorized users due to improper permission settings. It has Incorrect Access Control. |
| Git | 2.45.2 | CVE-2019-13010 | MEDIUM | 5.9 | An issue was discovered in GitLab Enterprise Edition 8.3 through 12.0.2. The color codes decoder was vulnerable to a resource depletion attack if specific formats were used. It allows Uncontrolled Resource Consumption.                                  |
| Git | 2.45.2 | CVE-2019-13011 | MEDIUM | 4.3 | An issue was discovered in GitLab Enterprise Edition 8.11.0 through 12.0.2. By using brute-force a user with access to a project, but not its repository could create a list of merge requests template names. It has excessive algorithmic complexity.     |
| Git | 2.45.2 | CVE-2019-13121 | HIGH   | 7.5 | An issue was discovered in GitLab Enterprise Edition 10.6 through 12.0.2. The GitHub project integration was vulnerable to an SSRF vulnerability which allowed an attacker to make requests to local network resources. It has Incorrect Access Control.    |
| Git | 2.45.2 | CVE-2020-10535 | MEDIUM | 5.3 | GitLab 12.8.x before 12.8.6, when sign-up is enabled, allows remote attackers to bypass email domain restrictions within the two-day grace period for an unconfirmed email address.   |
| Git | 2.45.2 | CVE-2020-10078 | MEDIUM | 6.1 | GitLab 12.1 through 12.8.1 allows XSS. The merge request submission form was determined to have a stored cross-site scripting vulnerability.  |
| Git | 2.45.2 | CVE-2020-10079 | MEDIUM | 5.3 | GitLab 7.10 through 12.8.1 has Incorrect Access Control. Under certain conditions where users should have been required to configure two-factor authentication, it was not being required.  |
| Git | 2.45.2 | CVE-2020-10080 | MEDIUM | 5.3 | GitLab 8.3 through 12.8.1 allows Information Disclosure. It was possible for certain non-members to access the Contribution Analytics page of a private group.  |
| Git | 2.45.2 | CVE-2020-10081 | MEDIUM | 6.5 | GitLab before 12.8.2 has Incorrect Access Control. It was internally discovered that the LFS import process could potentially be used to incorrectly access LFS objects not owned by the user.  |
| Git | 2.45.2 | CVE-2020-10082 | MEDIUM | 5.3 | GitLab 12.2 through 12.8.1 allows Denial of Service. A denial of service vulnerability impacting the designs for public issues was discovered.  |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2020-10083 | CRITICAL | 9.1 | GitLab 12.7 through 12.8.1 has Insecure Permissions. Under certain conditions involving groups, project authorization changes were not being applied.   |
| Git | 2.45.2 | CVE-2020-10084 | MEDIUM   | 5.3 | GitLab EE 11.6 through 12.8.1 allows Information Disclosure. Sending a specially crafted request to the vulnerability_feedback endpoint could result in the exposure of a private project namespace |
| Git | 2.45.2 | CVE-2020-10085 | MEDIUM   | 5.3 | GitLab 12.3.5 through 12.8.1 allows Information Disclosure. A particular view was exposing merge private merge request titles.  |
| Git | 2.45.2 | CVE-2020-10086 | MEDIUM   | 5.3 | GitLab 10.4 through 12.8.1 allows Directory Traversal. A particular endpoint was vulnerable to a directory traversal vulnerability, leading to arbitrary file read.                                 |
| Git | 2.45.2 | CVE-2020-10087 | HIGH     | 7.5 | GitLab before 12.8.2 allows Information Disclosure. Badge images were not being proxied, causing mixed content warnings as well as leaking the IP address of the user.                              |
| Git | 2.45.2 | CVE-2020-10088 | HIGH     | 8.1 | GitLab 12.5 through 12.8.1 has Insecure Permissions. Depending on particular group settings, it was possible for invited groups to be given the incorrect permission level.                         |
| Git | 2.45.2 | CVE-2020-10089 | HIGH     | 7.5 | GitLab 8.11 through 12.8.1 allows a Denial of Service when using several features to recursively request eachother,   |
| Git | 2.45.2 | CVE-2020-10090 | MEDIUM   | 5.3 | GitLab 11.7 through 12.8.1 allows Information Disclosure. Under certain group conditions, group epic information was unintentionally being disclosed.   |
| Git | 2.45.2 | CVE-2020-10091 | MEDIUM   | 6.1 | GitLab 9.3 through 12.8.1 allows XSS. A cross-site scripting vulnerability was found when viewing particular file types.  |
| Git | 2.45.2 | CVE-2020-10092 | MEDIUM   | 6.1 | GitLab 12.1 through 12.8.1 allows XSS. A cross-site scripting vulnerability was present in a particular view relating to the Grafana integration.   |
| Git | 2.45.2 | CVE-2020-10073 | HIGH     | 7.5 | GitLab EE 12.4.2 through 12.8.1 allows Denial of Service. It was internally discovered that a potential denial of service involving permissions checks could impact a project home page.            |
| Git | 2.45.2 | CVE-2020-10074 | CRITICAL | 9.8 | GitLab 10.1 through 12.8.1 has Incorrect Access Control. A scenario was discovered in which a GitLab account could be taken over through an expired link.   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2020-10075 | MEDIUM             | 6.1        | GitLab 12.5 through 12.8.1 allows HTML Injection. A particular error header was potentially susceptible to injection or potentially other vulnerabilities via unescaped input.  |
| Git | 2.45.2 | CVE-2020-10076 | MEDIUM             | 6.1        | GitLab 12.1 through 12.8.1 allows XSS. A stored cross-site scripting vulnerability was discovered when displaying merge requests.   |
| Git | 2.45.2 | CVE-2020-10077 | CRITICAL           | 9.8        | GitLab EE 3.0 through 12.8.1 allows SSRF. An internal investigation revealed that a particular deprecated service was creating a server side request forgery risk.  |
| Git | 2.45.2 | CVE-2020-5262  | ['HIGH', 'MEDIUM'] | [7.7, 5.5] | In EasyBuild before version 4.1.2, the GitHub Personal Access Token (PAT) used by EasyBuild for the GitHub integration features (like `--new-pr`, `--fro-pr`, etc.) is shown in plain text in EasyBuild debug log files. This issue is fixed in EasyBuild v4.1.2, and in the `master` + `develop` branches of the `easybuild-framework` repository.                   |
| Git | 2.45.2 | CVE-2020-10871 | MEDIUM             | 5.3        | In OpenWrt LuCI git-20.x, remote unauthenticated attackers can retrieve the list of installed packages and services. NOTE: the vendor disputes the significance of this report because, for instances reachable by an unauthenticated actor, the same information is available in other (more complex) ways, and there is no plan to restrict the information further |
| Git | 2.45.2 | CVE-2020-10952 | MEDIUM             | 6.5        | GitLab EE/CE 8.11 through 12.9.1 allows blocked users to pull/push docker images.   |
| Git | 2.45.2 | CVE-2020-10953 | HIGH               | 7.5        | In GitLab EE 11.7 through 12.9, the NPM feature is vulnerable to a path traversal issue.  |
| Git | 2.45.2 | CVE-2020-10954 | HIGH               | 7.5        | GitLab through 12.9 is affected by a potential DoS in repository archive download.  |
| Git | 2.45.2 | CVE-2020-10955 | MEDIUM             | 6.5        | GitLab EE/CE 11.1 through 12.9 is vulnerable to parameter tampering on an upload feature that allows an unauthorized user to read content available under specific folders.   |
| Git | 2.45.2 | CVE-2020-10956 | CRITICAL           | 9.8        | GitLab 8.10 and later through 12.9 is vulnerable to an SSRF in a project import note feature.   |
| Git | 2.45.2 | CVE-2020-7630  | CRITICAL           | 9.8        | git-add-remote through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the name argument.   |
| Git | 2.45.2 | CVE-2020-10975 | MEDIUM             | 4.3        | GitLab EE/CE 10.8 to 12.9 is leaking metadata and comments on vulnerabilities to unauthorized users on the vulnerability feedback page.   |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2020-10976 | HIGH     | 7.5 | GitLab EE/CE 8.17 to 12.9 is vulnerable to information leakage when querying a merge request widget.   |
| Git | 2.45.2 | CVE-2020-10977 | MEDIUM   | 5.5 | GitLab EE/CE 8.5 to 12.9 is vulnerable to a path traversal when moving an issue between projects.  |
| Git | 2.45.2 | CVE-2020-10978 | MEDIUM   | 5.3 | GitLab EE/CE 8.11 to 12.9 is leaking information on Issues opened in a public project and then moved to a private project through Web-UI and GraphQL API.  |
| Git | 2.45.2 | CVE-2020-10979 | MEDIUM   | 4.3 | GitLab EE/CE 11.10 to 12.9 is leaking information on restricted CI pipelines metrics to unauthorized users.  |
| Git | 2.45.2 | CVE-2020-10980 | CRITICAL | 9.8 | GitLab EE/CE 8.0.rc1 to 12.9 is vulnerable to a blind SSRF in the FogBugz integration.   |
| Git | 2.45.2 | CVE-2020-10981 | MEDIUM   | 4.3 | GitLab EE/CE 9.0 to 12.9 allows a maintainer to modify other maintainers' pipeline trigger descriptions within the same project.   |
| Git | 2.45.2 | CVE-2018-21034 | MEDIUM   | 6.5 | In Argo versions prior to v1.5.0-rc1, it was possible for authenticated Argo users to submit API calls to retrieve secrets and other manifests which were stored within git.   |
| Git | 2.45.2 | CVE-2020-11710 | CRITICAL | 9.8 | <p>An issue was discovered in docker-kong (for Kong) through 2.0.3. The admin API port may be accessible on interfaces other than 127.0.0.1.</p> <p>NOTE: The vendor argue that this CVE is not a vulnerability because it has an inaccurate bug scope and patch links. 1) Inaccurate Bug Scope - The issue scope was on Kong's docker-compose template, and not Kong's docker image itself. In reality, this issue is not associated with any version of the Kong gateway. As such, the description stating "An issue was discovered in docker-kong (for Kong) through 2.0.3." is incorrect. This issue only occurs if a user decided to spin up Kong via docker-compose without following the security documentation. The docker-compose template is meant for users to quickly get started with Kong, and is meant for development purposes only. 2) Incorrect Patch Links - The CVE currently points to a documentation improvement as a "Patch" link: <a href="https://github.com/Kong/docs.konghq.com/commit/d693827c32144943a2f45abc01...">https://github.com/Kong/docs.konghq.com/commit/d693827c32144943a2f45abc01...</a></p> |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-5260  | ['CRITICAL', 'HIGH'] | [9.3, 7.5] | Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that contain an encoded newline can inject unintended values into the credential helper protocol stream, causing the credential helper to retrieve the password for one server (e.g., good.example.com) for an HTTP request being made to another server (e.g., evil.example.com), resulting in credentials for the former being sent to the latter. There are no restrictions on the relationship between the two, meaning that an attacker can craft a URL that will present stored credentials for any host to a host of their choosing. The vulnerability can be triggered by feeding a malicious URL to git clone. However, the affected URLs look rather suspicious; the likely vector would be... |
| Git | 2.45.2 | CVE-2020-11008 | ['MEDIUM', 'HIGH']   | [4.0, 7.5] | Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where _some_ credential is leaked (but the attacker cannot control which one). Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently published Git versions can cause Git to send a "blank" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching _any_ URL, and will return some unspecified stored password, leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to `git clone`. However, the affected URLs look rather suspicious; the likely vector would be through sy... |
| Git | 2.45.2 | CVE-2020-11505 | HIGH                 | 7.5        | An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling.  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2020-11506 | HIGH                 | 7.5        | An issue was discovered in GitLab 10.7.0 and later through 12.9.2. A Workhorse bypass could lead to job artifact uploads and file disclosure (Exposure of Sensitive Information) via request smuggling.   |
| Git | 2.45.2 | CVE-2020-11649 | MEDIUM               | 6.5        | An issue was discovered in GitLab CE and EE 8.15 through 12.9.2. Members of a group could still have access after the group is deleted.   |
| Git | 2.45.2 | CVE-2020-12275 | MEDIUM               | 5.3        | GitLab 12.6 through 12.9 is vulnerable to a privilege escalation that allows an external user to create a personal snippet through the API.   |
| Git | 2.45.2 | CVE-2020-12276 | MEDIUM               | 4.8        | GitLab 9.5.9 through 12.9 is vulnerable to stored XSS in an admin notification feature.   |
| Git | 2.45.2 | CVE-2020-12277 | MEDIUM               | 5.3        | GitLab 10.8 through 12.9 has a vulnerability that allows someone to mirror a repository even if the feature is not activated.   |
| Git | 2.45.2 | CVE-2020-12448 | MEDIUM               | 5.3        | GitLab EE 12.8 and later allows Exposure of Sensitive Information to an Unauthorized Actor via NuGet.   |
| Git | 2.45.2 | CVE-2020-13246 | HIGH                 | 7.5        | An issue was discovered in Gitea through 1.11.5. An attacker can trigger a deadlock by initiating a transfer of a repository's ownership from one organization to another.  |
| Git | 2.45.2 | CVE-2020-7651  | MEDIUM               | 4.3        | All versions of snyk-broker before 4.79.0 are vulnerable to Arbitrary File Read. It allows partial file reads for users who have access to Snyk's internal network via patch history from GitHub Commits API.   |
| Git | 2.45.2 | CVE-2020-10516 | CRITICAL             | 9.8        | An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20. This vulnerability was reported via the GitHub Bug Bounty program. |
| Git | 2.45.2 | CVE-2020-13266 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Insecure authorization in Project Deploy Keys in GitLab CE/EE 12.8 and later through 13.0.1 allows users to update permissions of other users' deploy keys under certain conditions   |
| Git | 2.45.2 | CVE-2020-13267 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | A Stored Cross-Site Scripting vulnerability allowed the execution on Javascript payloads on the Metrics Dashboard in GitLab CE/EE 12.8 and later through 13.0.1   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-13268 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | A specially crafted request could be used to confirm the existence of files hosted on object storage services, without disclosing their contents. This vulnerability affects GitLab CE/EE 12.10 and later through 13.0.1   |
| Git | 2.45.2 | CVE-2020-13269 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | A Reflected Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code on the Static Site Editor in GitLab CE/EE 12.10 and later through 13.0.1   |
| Git | 2.45.2 | CVE-2020-13270 | ['HIGH', 'HIGH']     | [7.5, 8.8] | Missing permission check on fork relation creation in GitLab CE/EE 11.3 and later through 13.0.1 allows guest users to create a fork relation on restricted public projects via API  |
| Git | 2.45.2 | CVE-2020-13271 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | A Stored Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code in the blobs API in all previous GitLab CE/EE versions through 13.0.1   |
| Git | 2.45.2 | CVE-2020-4059  | ['HIGH', 'HIGH']     | [7.3, 7.3] | In mversion before 2.0.0, there is a command injection vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This vulnerability is patched by version 2.0.0. Previous releases are deprecated in npm. As a workaround, make sure to escape git commit messages when using the commitMessage option for the update function. |
| Git | 2.45.2 | CVE-2019-20864 | HIGH                 | 7.5        | An issue was discovered in Mattermost Plugins before 5.13.0. The GitHub plugin allows an attacker to attach his Mattermost account to a different person's GitHub account.   |
| Git | 2.45.2 | CVE-2020-13277 | ['MEDIUM', 'MEDIUM'] | [6.3, 6.5] | An authorization issue in the mirroring logic allowed read access to private repositories in GitLab CE/EE 10.6 and later through 13.0.5  |
| Git | 2.45.2 | CVE-2020-13262 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | Client-Side code injection through Mermaid markup in GitLab CE/EE 12.9 and later through 13.0.1 allows a specially crafted Mermaid payload to PUT requests on behalf of other users via clicking on a link   |
| Git | 2.45.2 | CVE-2020-13265 | ['MEDIUM', 'MEDIUM'] | [4.3, 5.3] | User email verification bypass in GitLab CE/EE 12.5 and later through 13.0.1 allows user to bypass email verification  |
| Git | 2.45.2 | CVE-2020-13273 | ['HIGH', 'HIGH']     | [7.5, 7.5] | A Denial of Service vulnerability allowed exhausting the system resources in GitLab CE/EE 12.0 and later through 13.0.1  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-13274 | ['HIGH', 'HIGH']     | [7.5, 7.5] | A security issue allowed achieving Denial of Service attacks through memory exhaustion by uploading malicious artifacts in all previous GitLab versions through 13.0.1   |
| Git | 2.45.2 | CVE-2020-13275 | ['HIGH', 'HIGH']     | [8.0, 8.1] | A user with an unverified email address could request an access to domain restricted groups in GitLab EE 12.2 and later through 13.0.1   |
| Git | 2.45.2 | CVE-2020-13276 | ['HIGH', 'MEDIUM']   | [7.4, 4.3] | User is allowed to set an email as a notification email even without verifying the new email in all previous GitLab CE/EE versions through 13.0.1  |
| Git | 2.45.2 | CVE-2020-13261 | ['MEDIUM', 'LOW']    | [5.3, 2.7] | Amazon EKS credentials disclosure in GitLab CE/EE 12.6 and later through 13.0.1 allows other administrators to view Amazon EKS credentials via HTML source code  |
| Git | 2.45.2 | CVE-2020-13263 | ['HIGH', 'HIGH']     | [7.5, 8.8] | An authorization issue relating to project maintainer impersonation was identified in GitLab EE 9.5 and later through 13.0.1 that could allow unauthorized users to impersonate as a maintainer to perform limited actions.  |
| Git | 2.45.2 | CVE-2020-13264 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Kubernetes cluster token disclosure in GitLab CE/EE 10.3 and later through 13.0.1 allows other group maintainers to view Kubernetes cluster token  |
| Git | 2.45.2 | CVE-2020-13279 | ['HIGH', 'HIGH']     | [8.6, 8.6] | Client side code execution in gitlab-vscode-extension v2.2.0 allows attacker to execute code on user system  |
| Git | 2.45.2 | CVE-2020-7664  | ['HIGH', 'HIGH']     | [7.5, 7.5] | In all versions of the package github.com/unknwon/cae/zip, the ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide.   |
| Git | 2.45.2 | CVE-2020-7668  | ['HIGH', 'HIGH']     | [7.5, 7.5] | In all versions of the package github.com/unknwon/cae/tz, the ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide.  |
| Git | 2.45.2 | CVE-2020-7667  | ['HIGH', 'HIGH']     | [7.5, 7.5] | In package github.com/sassoftware/go-rpmutils/cpio before version 0.1.0, the CPIO extraction functionality doesn't sanitize the paths of the archived files for leading and non-leading ".." which leads in file extraction outside of the current directory. Note: the fixing commit was applied to all affected versions which were re-released. |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2020-5238  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | The table extension in GitHub Flavored Markdown before version 0.29.0.gfm.1 takes $O(n * n)$ time to parse certain inputs. An attacker could craft a markdown table which would take an unreasonably long time to process, causing a denial of service. This issue does not affect the upstream cmark project. The issue has been fixed in version 0.29.0.gfm.1.  |
| Git | 2.45.2 | CVE-2020-2212  | MEDIUM               | 4.3        | Jenkins GitHub Coverage Reporter Plugin 1.8 and earlier stores secrets unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system or read permissions on the system configuration.  |
| Git | 2.45.2 | CVE-2020-15525 | MEDIUM               | 5.3        | GitLab EE 11.3 through 13.1.2 has Incorrect Access Control because of the Maven package upload endpoint.  |
| Git | 2.45.2 | CVE-2020-2228  | HIGH                 | 8.8        | Jenkins Gitlab Authentication Plugin 1.5 and earlier does not perform group authorization checks properly, resulting in a privilege escalation vulnerability.   |
| Git | 2.45.2 | CVE-2020-14001 | CRITICAL             | 9.8        | The kramdown gem before 2.3.0 for Ruby processes the template option inside Kramdown documents by default, which allows unintended read access (such as template="/etc/passwd") or unintended embedded Ruby code execution (such as a string that begins with template="string://<%= "). NOTE: kramdown is used in Jekyll, GitLab Pages, GitHub Pages, and Thredded Forum.  |
| Git | 2.45.2 | CVE-2020-15133 | ['HIGH', 'HIGH']     | [8.0, 8.7] | In faye-websocket before version 0.11.0, there is a lack of certification validation in TLS handshakes. The `Faye::WebSocket::Client` class uses the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `wss:` connection made using this library is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. For further background information on this issue, please see the referenced GitHub Advisory. Upgrading `faye-websocket` to v0.11.0 is recommended. |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2020-15134 | ['HIGH', 'HIGH']         | [8.0, 8.7] | Faye before version 1.4.0, there is a lack of certification validation in TLS handshakes. Faye uses em-http-request and faye-websocket in the Ruby version of its client. Those libraries both use the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `https:` or `wss:` connection made using these libraries is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. The first request a Faye client makes is always sent via normal HTTP, but later messages may be sent via WebSocket. Therefore it is vulnerable to the same problem that these underlying libraries are, and we needed both libraries to support TLS verification before Faye could claim to d... |
| Git | 2.45.2 | CVE-2020-13292 | ['CRITICAL', 'CRITICAL'] | [9.6, 9.6] | In GitLab before 13.0.12, 13.1.6 and 13.2.3, it is possible to bypass E-mail verification which is required for OAuth Flow.  |
| Git | 2.45.2 | CVE-2020-13293 | ['MEDIUM', 'HIGH']       | [6.3, 7.1] | In GitLab before 13.0.12, 13.1.6 and 13.2.3 using a branch with a hexadecimal name could override an existing hash.  |
| Git | 2.45.2 | CVE-2020-13294 | ['MEDIUM', 'MEDIUM']     | [4.2, 5.4] | In GitLab before 13.0.12, 13.1.6 and 13.2.3, access grants were not revoked when a user revoked access to an application.  |
| Git | 2.45.2 | CVE-2020-13295 | ['MEDIUM', 'HIGH']       | [5.4, 8.8] | For GitLab Runner before 13.0.12, 13.1.6, 13.2.3, by replacing dockerd with a malicious server, the Shared Runner is susceptible to SSRF.  |
| Git | 2.45.2 | CVE-2020-2237  | MEDIUM                   | 4.3        | A cross-site request forgery (CSRF) vulnerability in Jenkins Flaky Test Handler Plugin 1.0.4 and earlier allows attackers to rebuild a project at a previous git revision.   |
| Git | 2.45.2 | CVE-2020-13288 | ['MEDIUM', 'MEDIUM']     | [5.5, 4.8] | In GitLab before 13.0.12, 13.1.6, and 13.2.3, a stored XSS vulnerability exists in the CI/CD Jobs page   |
| Git | 2.45.2 | CVE-2020-13290 | ['HIGH', 'HIGH']         | [7.5, 7.2] | In GitLab before 13.0.12, 13.1.6, and 13.2.3, improper access control was used on the Applications page  |
| Git | 2.45.2 | CVE-2020-13291 | ['HIGH', 'HIGH']         | [8.1, 8.1] | In GitLab before 13.2.3, project sharing could temporarily allow too permissive access.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-5415  | CRITICAL             | 10.0       | Concourse, versions prior to 6.3.1 and 6.4.1, in installations which use the GitLab auth connector, is vulnerable to identity spoofing by way of configuring a GitLab account with the same full name as another user who is granted access to a Concourse team. GitLab groups do not have this vulnerability, so GitLab users may be moved into groups which are then configured in the Concourse team.   |
| Git | 2.45.2 | CVE-2020-13280 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | For GitLab before 13.0.12, 13.1.6, 13.2.3 a memory exhaustion flaw exists due to excessive logging of an invite email error message.   |
| Git | 2.45.2 | CVE-2020-13282 | ['LOW', 'LOW']       | [3.1, 3.5] | For GitLab before 13.0.12, 13.1.6, 13.2.3 after a group transfer occurs, members from a parent group keep their access level on the subgroup leading to improper access.   |
| Git | 2.45.2 | CVE-2020-13283 | ['HIGH', 'MEDIUM']   | [7.3, 5.4] | For GitLab before 13.0.12, 13.1.6, 13.2.3 a cross-site scripting vulnerability exists in the issues list via milestone title.  |
| Git | 2.45.2 | CVE-2020-13285 | ['HIGH', 'MEDIUM']   | [7.3, 5.4] | For GitLab before 13.0.12, 13.1.6, 13.2.3 a cross-site scripting (XSS) vulnerability exists in the issue reference number tooltip.   |
| Git | 2.45.2 | CVE-2020-13281 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | For GitLab before 13.0.12, 13.1.6, 13.2.3 a denial of service exists in the project import feature   |
| Git | 2.45.2 | CVE-2020-13286 | ['MEDIUM', 'MEDIUM'] | [6.4, 4.3] | For GitLab before 13.0.12, 13.1.6, 13.2.3 user controlled git configuration settings can be modified to result in Server Side Request Forgery.   |
| Git | 2.45.2 | CVE-2020-9708  | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | The resolveRepositoryPath function doesn't properly validate user input and a malicious user may traverse to any valid Git repository outside the repoRoot. This issue may lead to unauthorized access of private Git repositories as long as the malicious user knows or brute-forces the location of the repository.   |
| Git | 2.45.2 | CVE-2020-7711  | ['HIGH', 'HIGH']     | [7.5, 7.5] | This affects all versions of package <a href="https://github.com/russellhaering/goxmldsig">github.com/russellhaering/goxmldsig</a> . There is a crash on nil-pointer dereference caused by sending malformed XML signatures.   |
| Git | 2.45.2 | CVE-2020-10517 | MEDIUM               | 4.3        | An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to determine the names of unauthorized private repositories given their numerical IDs. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in versions 2.21.6, 2.20.15, and 2.19.21. This vulnerability was reported via the GitHub Bug Bounty program. |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2020-10518 | HIGH                     | 8.8        | A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in 2.21.6, 2.20.15, and 2.19.21. The underlying issues contributing to this vulnerability were identified both internally and through the GitHub Security Bug Bounty program. |
| Git | 2.45.2 | CVE-2020-15165 | ['CRITICAL', 'CRITICAL'] | [9.3, 9.1] | Version 1.1.6-free of Chameleon Mini Live Debugger on Google Play Store may have had its sources or permissions tampered by a malicious actor. The official maintainer of the package is recommending all users upgrade to v1.1.8 as soon as possible. For more information, review the referenced GitHub Security Advisory.   |
| Git | 2.45.2 | CVE-2020-2238  | MEDIUM                   | 5.4        | Jenkins Git Parameter Plugin 0.9.12 and earlier does not escape the repository field on the 'Build with Parameters' page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.   |
| Git | 2.45.2 | CVE-2020-7665  | ['HIGH', 'HIGH']         | [7.5, 7.5] | This affects all versions of package github.com/u-root/u-root/pkg/uzip. It is vulnerable to both leading and non-leading relative path traversal attacks in zip file extraction.   |
| Git | 2.45.2 | CVE-2020-7666  | ['HIGH', 'HIGH']         | [7.5, 7.5] | This affects all versions of package github.com/u-root/u-root/pkg/cpio. It is vulnerable to leading, non-leading relative path traversal attacks and symlink based (relative and absolute) path traversal attacks in cpio file extraction.   |
| Git | 2.45.2 | CVE-2020-7669  | HIGH                     | 7.5        | This affects all versions of package github.com/u-root/u-root/pkg/tarutil. It is vulnerable to both leading and non-leading relative path traversal attacks in tar file extraction.  |
| Git | 2.45.2 | CVE-2020-15167 | ['HIGH', 'HIGH']         | [8.2, 8.6] | In Miller (command line utility) using the configuration file support introduced in version 5.9.0, it is possible for an attacker to cause Miller to run arbitrary code by placing a malicious <code>.mlrrc`</code> file in the working directory. See linked GitHub Security Advisory for complete details. A fix is ready and will be released as Miller 5.9.1.  |

|     |        |                |                        |             |   |
|-----|--------|----------------|------------------------|-------------|---|
| Git | 2.45.2 | CVE-2020-13284 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. API Authorization Using Outdated CI Job Token  |
| Git | 2.45.2 | CVE-2020-13287 | ['MEDIUM', 'MEDIUM']   | [4.3, 4.3]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Project reporters and above could see confidential EPIC attached to confidential issues  |
| Git | 2.45.2 | CVE-2020-13289 | ['MEDIUM', 'MEDIUM']   | [5.4, 5.4]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. In certain cases an invalid username could be accepted when 2FA is activated.  |
| Git | 2.45.2 | CVE-2020-13299 | ['HIGH', 'HIGH']       | [8.1, 8.1]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. The revocation feature was not revoking all session tokens and one could re-use it to obtain a valid session.                  |
| Git | 2.45.2 | CVE-2020-13300 | ['HIGH', 'CRITICAL']   | [8.0, 10.0] | GitLab CE/EE version 13.3 prior to 13.3.4 was vulnerable to an OAuth authorization scope change without user consent in the middle of the authorization flow.   |
| Git | 2.45.2 | CVE-2020-13316 | ['MEDIUM', 'MEDIUM']   | [5.4, 4.3]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not validating a Deploy-Token and allowed a disabled repository be accessible via a git command line.               |
| Git | 2.45.2 | CVE-2020-13318 | ['MEDIUM', 'HIGH']     | [6.4, 7.3]  | A vulnerability was discovered in GitLab versions before 13.0.12, 13.1.10, 13.2.8 and 13.3.4. GitLabs EKS integration was vulnerable to a cross-account assume role attack.   |
| Git | 2.45.2 | CVE-2020-13311 | ['MEDIUM', 'MEDIUM']   | [4.3, 4.3]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Wiki was vulnerable to a parser attack that prohibits anyone from accessing the Wiki functionality through the user interface. |
| Git | 2.45.2 | CVE-2020-13312 | ['MEDIUM', 'CRITICAL'] | [6.5, 9.8]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab OAuth endpoint was vulnerable to brute-force attacks through a specific parameter.                                      |
| Git | 2.45.2 | CVE-2020-13313 | ['MEDIUM', 'MEDIUM']   | [4.3, 4.3]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. An unauthorized project maintainer could edit the subgroup badges due to the lack of authorization control.                    |
| Git | 2.45.2 | CVE-2020-13314 | ['LOW', 'MEDIUM']      | [3.7, 5.3]  | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab Omniauth endpoint allowed a malicious user to submit content to be displayed back to the user within error messages.    |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2020-13317 | ['MEDIUM', 'MEDIUM'] | [6.5, 4.9] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8, and 13.3.4. An insufficient check in the GraphQL api allowed a maintainer to delete a repository.   |
| Git | 2.45.2 | CVE-2020-13297 | ['LOW', 'MEDIUM']    | [3.8, 5.4] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. When 2 factor authentication was enabled for groups, a malicious user could bypass that restriction by sending a specific query to the API endpoint. |
| Git | 2.45.2 | CVE-2020-13298 | ['HIGH', 'MEDIUM']   | [7.2, 5.8] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Conan package upload functionality was not properly validating the supplied parameters, which resulted in the limited files disclosure.              |
| Git | 2.45.2 | CVE-2020-13301 | ['MEDIUM', 'MEDIUM'] | [5.5, 4.8] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was vulnerable to a stored XSS on the standalone vulnerability page.  |
| Git | 2.45.2 | CVE-2020-13302 | ['LOW', 'HIGH']      | [3.8, 7.2] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Under certain conditions GitLab was not properly revoking user sessions and allowed a malicious user to access a user account with an old password.  |
| Git | 2.45.2 | CVE-2020-13304 | ['LOW', 'HIGH']      | [3.8, 7.2] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Same 2 factor Authentication secret code was generated which resulted an attacker to maintain access under certain conditions.                       |
| Git | 2.45.2 | CVE-2020-13305 | ['LOW', 'MEDIUM']    | [3.5, 4.3] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not invalidating project invitation link upon removing a user from a project.   |
| Git | 2.45.2 | CVE-2020-13306 | ['LOW', 'HIGH']      | [3.7, 7.5] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab Webhook feature could be abused to perform denial of service attacks due to the lack of rate limitation.                                      |
| Git | 2.45.2 | CVE-2020-13309 | ['MEDIUM', 'HIGH']   | [5.4, 8.8] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was vulnerable to a blind SSRF attack through the repository mirroring feature.   |
| Git | 2.45.2 | CVE-2020-13310 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | A vulnerability was discovered in GitLab runner versions before 13.1.3, 13.2.3 and 13.3.1. It was possible to make the gitlab-runner process crash by sending malformed queries, resulting in a denial of service.                        |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-13315 | ['LOW', 'HIGH']      | [3.7, 7.5] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. The profile activity page was not restricting the amount of results one could request, potentially resulting in a denial of service.  |
| Git | 2.45.2 | CVE-2020-13303 | ['HIGH', 'MEDIUM']   | [7.1, 6.5] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Due to improper verification of permissions, an unauthorized user can access a private repository within a public project.  |
| Git | 2.45.2 | CVE-2020-13307 | ['LOW', 'MEDIUM']    | [3.8, 4.7] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not revoking current user sessions when 2 factor authentication was activated allowing a malicious user to maintain their access.  |
| Git | 2.45.2 | CVE-2020-13308 | ['LOW', 'LOW']       | [2.7, 2.7] | A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. A user without 2 factor authentication enabled could be prohibited from accessing GitLab by being invited into a project that had 2 factor authentication inheritance.  |
| Git | 2.45.2 | CVE-2020-15187 | ['LOW', 'MEDIUM']    | [3.0, 4.7] | In Helm before versions 2.16.11 and 3.3.2, a Helm plugin can contain duplicates of the same entry, with the last one always used. If a plugin is compromised, this lowers the level of access that an attacker needs to modify a plugin's install hooks, causing a local execution attack. To perform this attack, an attacker must have write access to the git repository or plugin archive (.tgz) while being downloaded (which can occur during a MITM attack on a non-SSL connection). This issue has been patched in Helm 2.16.11 and Helm 3.3.2. As a possible workaround make sure to install plugins using a secure connection protocol like SSL. |
| Git | 2.45.2 | CVE-2020-13296 | ['MEDIUM', 'HIGH']   | [6.5, 8.8] | An issue has been discovered in GitLab affecting versions $\geq 10.7 < 13.0.14$ , $\geq 13.1.0 < 13.1.8$ , $\geq 13.2.0 < 13.2.6$ . Improper Access Control for Deploy Tokens  |
| Git | 2.45.2 | CVE-2020-13319 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting versions prior to 13.1.2, 13.0.8 and 12.10.13. Missing permission check for adding time spent on an issue.  |
| Git | 2.45.2 | CVE-2020-13320 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An issue has been discovered in GitLab before version 12.10.13 that allowed a project member with limited permissions to view the project security dashboard.  |
| Git | 2.45.2 | CVE-2020-13321 | ['HIGH', 'HIGH']     | [8.3, 8.3] | A vulnerability was discovered in GitLab versions prior to 13.1. Username format restrictions could be bypassed allowing for html tags to be added.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-13322 | ['HIGH', 'HIGH']     | [7.2, 7.2] | A vulnerability was discovered in GitLab versions after 12.9. Due to improper verification of permissions, an unauthorized user can create and delete deploy tokens.                           |
| Git | 2.45.2 | CVE-2020-13323 | ['HIGH', 'HIGH']     | [7.7, 7.7] | A vulnerability was discovered in GitLab versions prior 13.1. Under certain conditions private merge requests could be read via Todos  |
| Git | 2.45.2 | CVE-2020-13324 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | A vulnerability was discovered in GitLab versions prior to 13.1. Under certain conditions the private activity of a user could be exposed via the API.   |
| Git | 2.45.2 | CVE-2020-13325 | ['HIGH', 'HIGH']     | [7.1, 7.1] | A vulnerability was discovered in GitLab versions prior 13.1. The comment section of the issue page was not restricting the characters properly, potentially resulting in a denial of service. |
| Git | 2.45.2 | CVE-2020-13326 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | A vulnerability was discovered in GitLab versions prior to 13.1. Under certain conditions the restriction for Github project import could be bypassed.   |
| Git | 2.45.2 | CVE-2020-13328 | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | An issue has been discovered in GitLab affecting versions prior to 13.1.2, 13.0.8 and 12.10.13. GitLab was vulnerable to a stored XSS by using the PyPi files API.                             |
| Git | 2.45.2 | CVE-2020-13329 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An issue has been discovered in GitLab affecting versions from 12.6.2 prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the blob view feature.                                    |
| Git | 2.45.2 | CVE-2020-13330 | ['MEDIUM', 'MEDIUM'] | [4.4, 5.4] | An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS in import the Bitbucket project feature.                                    |
| Git | 2.45.2 | CVE-2020-13331 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the Wiki pasges.  |
| Git | 2.45.2 | CVE-2020-13336 | ['MEDIUM', 'MEDIUM'] | [4.0, 4.8] | An issue has been discovered in GitLab affecting versions from 11.8 before 12.10.13. GitLab was vulnerable to a stored XSS by in the error tracking feature.                                   |
| Git | 2.45.2 | CVE-2020-13337 | ['HIGH', 'MEDIUM']   | [7.2, 4.8] | An issue has been discovered in GitLab affecting versions from 12.10 to 12.10.12 that allowed for a stored XSS payload to be added as a group name.  |
| Git | 2.45.2 | CVE-2020-13338 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | An issue has been discovered in GitLab affecting versions prior to 12.10.13, 13.0.8, 13.1.2. A stored cross-site scripting vulnerability was discovered when editing references.               |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2020-15236 | ['HIGH', 'HIGH']     | [8.6, 7.5] | In Wiki.js before version 2.5.151, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit 084dcd69d1591586ee4752101e675d5f0ac6dcdc fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any directory traversal (e.g. `..` and `.`) sequences as well as invalid filesystem characters from the path. As a workaround, disable any storage module with local asset caching capabilities such as Local File System and Git. |
| Git | 2.45.2 | CVE-2020-13333 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | A potential DOS vulnerability was discovered in GitLab versions 13.1, 13.2 and 13.3. The api to update an asset as a link from a release had a regex check which caused exponential number of backtracks for certain user supplied values resulting in high CPU usage.  |
| Git | 2.45.2 | CVE-2020-13343 | ['HIGH', 'HIGH']     | [7.5, 8.8] | An issue has been discovered in GitLab affecting all versions starting from 11.2. Unauthorized Users Can View Custom Project Template   |
| Git | 2.45.2 | CVE-2020-13345 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.4] | An issue has been discovered in GitLab affecting all versions starting from 10.8. Reflected XSS on Multiple Routes  |
| Git | 2.45.2 | CVE-2020-13334 | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | In GitLab versions prior to 13.2.10, 13.3.7 and 13.4.2, improper authorization checks allow a non-member of a project/group to change the confidentiality attribute of issue via mutation GraphQL query   |
| Git | 2.45.2 | CVE-2020-13335 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper group membership validation when deleting a user account in GitLab >=7.12 allows a user to delete own account without deleting/transferring their group.   |
| Git | 2.45.2 | CVE-2020-13346 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Membership changes are not reflected in ToDo subscriptions in GitLab versions prior to 13.2.10, 13.3.7 and 13.4.2, allowing guest users to access confidential issues through API.  |

|     |        |                |                          |            |   |
|-----|--------|----------------|--------------------------|------------|---|
| Git | 2.45.2 | CVE-2020-13347 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.1] | A command injection vulnerability was discovered in Gitlab runner versions prior to 13.2.4, 13.3.2 and 13.4.1. When the runner is configured on a Windows system with a docker executor, which allows the attacker to run arbitrary commands on Windows host, via DOCKER_AUTH_CONFIG build variable.  |
| Git | 2.45.2 | CVE-2020-13342 | ['LOW', 'LOW']           | [2.7, 2.7] | An issue has been discovered in GitLab affecting versions prior to 13.2.10, 13.3.7 and 13.4.2: Lack of Rate Limiting at Re-Sending Confirmation Email   |
| Git | 2.45.2 | CVE-2020-13339 | ['MEDIUM', 'MEDIUM']     | [5.5, 6.5] | An issue has been discovered in GitLab affecting all versions before 13.2.10, 13.3.7 and 13.4.2: XSS in SVG File Preview. Overall impact is limited due to the current user only being impacted.  |
| Git | 2.45.2 | CVE-2020-13340 | ['HIGH', 'HIGH']         | [8.7, 8.7] | An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2: Stored XSS in CI Job Log   |
| Git | 2.45.2 | CVE-2020-13344 | ['MEDIUM', 'MEDIUM']     | [5.7, 4.4] | An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2. Sessions keys are stored in plain-text in Redis which allows attacker with Redis access to authenticate as any user that has a session stored in Redis   |
| Git | 2.45.2 | CVE-2020-13341 | ['MEDIUM', 'MEDIUM']     | [4.9, 4.9] | An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2. Insufficient permission check allows attacker with developer role to perform various deletions.  |
| Git | 2.45.2 | CVE-2020-15250 | ['MEDIUM', 'MEDIUM']     | [4.4, 5.5] | In JUnit4 from version 4.7 and before 4.13.1, the test rule TemporaryFolder contains a local information disclosure vulnerability. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. This vulnerability impacts you if the JUnit tests write sensitive information, like API keys or passwords, into the temporary folder, and the JUnit tests execute in an environment where the OS has other untrusted users. Because certain JDK file system APIs were only added in JDK 1.7, this fix is dependent upon the version of the JDK you are using. For Java 1.7 and higher users: this vulnerability is fixed in 4.13.1. For Java 1.6 and lower users: no patch i... |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2020-21674 | MEDIUM             | 6.5        | Heap-based buffer overflow in archive_string_append_from_wcs() (archive_string.c) in libarchive-3.4.1dev allows remote attackers to cause a denial of service (out-of-bounds write in heap memory resulting into a crash) via a crafted archive file. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected.  |
| Git | 2.45.2 | CVE-2020-14144 | HIGH               | 7.2        | The git hook feature in Gitea 1.1.0 through 1.12.5 might allow for authenticated remote code execution in customer environments where the documentation was not understood (e.g., one viewpoint is that the dangerousness of this feature should be documented immediately above the ENABLE_GIT_HOOKS line in the config file). NOTE: The vendor has indicated this is not a vulnerability and states "This is a functionality of the software that is limited to a very limited subset of accounts. If you give someone the privilege to execute arbitrary code on your server, they can execute arbitrary code on your server. We provide very clear warnings to users around this functionality and what it provides. |
| Git | 2.45.2 | CVE-2020-15867 | HIGH               | 7.2        | The git hook feature in Gogs 0.5.5 through 0.12.2 allows for authenticated remote code execution. There can be a privilege escalation if access to this hook feature is granted to a user who does not have administrative privileges. NOTE: because this is mentioned in the documentation but not in the UI, it could be considered a "Product UI does not Warn User of Unsafe Actions" issue.   |
| Git | 2.45.2 | CVE-2020-13327 | ['MEDIUM', 'HIGH'] | [6.0, 7.5] | An issue has been discovered in GitLab Runner affecting all versions starting from 13.4.0 before 13.4.2, all versions starting from 13.3.0 before 13.3.7, all versions starting from 13.2.0 before 13.2.10. Insecure Runner Configuration in Kubernetes Environments   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-15272 | ['HIGH', 'CRITICAL'] | [8.7, 9.6] | In the git-tag-annotation-action (open source GitHub Action) before version 1.0.1, an attacker can execute arbitrary (*) shell commands if they can control the value of [the `tag` input] or manage to alter the value of [the `GITHUB_REF` environment variable]. The problem has been patched in version 1.0.1. If you don't use the `tag` input you are most likely safe. The `GITHUB_REF` environment variable is protected by the GitHub Actions environment so attacks from there should be impossible. If you must use the `tag` input and cannot upgrade to `> 1.0.0` make sure that the value is not controlled by another Action. |
| Git | 2.45.2 | CVE-2020-27986 | ['HIGH', 'HIGH']     | [7.5, 7.5] | SonarQube 8.4.2.36762 allows remote attackers to discover cleartext SMTP, SVN, and GitLab credentials via the api/settings/values URI. NOTE: reportedly, the vendor's position for SMTP and SVN is "it is the administrator's responsibility to configure it.  |
| Git | 2.45.2 | CVE-2020-27955 | CRITICAL             | 9.8        | Git LFS 2.12.0 allows Remote Code Execution.   |
| Git | 2.45.2 | CVE-2020-14188 | CRITICAL             | 9.8        | The preprocessArgs function in the Atlassian gajira-create GitHub Action before version 2.0.1 allows remote attackers to execute arbitrary code in the context of a GitHub runner by creating a specially crafted GitHub issue.  |
| Git | 2.45.2 | CVE-2020-14189 | CRITICAL             | 9.8        | The execute function in in the Atlassian gajira-comment GitHub Action before version 2.0.2 allows remote attackers to execute arbitrary code in the context of a GitHub runner by creating a specially crafted GitHub issue comment.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-26230 | ['HIGH', 'MEDIUM']   | [7.4, 5.3] | Radar COVID is the official COVID-19 exposure notification app for Spain. In affected versions of Radar COVID, identification and de-anonymization of COVID-19 positive users that upload Radar COVID TEKs to the Radar COVID server is possible. This vulnerability enables the identification and de-anonymization of COVID-19 positive users when using Radar COVID. The vulnerability is caused by the fact that Radar COVID connections to the server (uploading of TEKs to the backend) are only made by COVID-19 positives. Therefore, any on-path observer with the ability to monitor traffic between the app and the server can identify which users had a positive test. Such an adversary can be the mobile network operator (MNO) if the connection is done through a mobile network, the Internet Service Provider (ISP) if the connection is done through the Internet (e.g., a home network), a VPN provider used by the user, the local network operator in the case of enterprise networks, or any eavesdropper wit... |
| Git | 2.45.2 | CVE-2020-13352 | ['LOW', 'MEDIUM']    | [3.7, 5.3] | Private group info is leaked leaked in GitLab CE/EE version 10.2 and above, when the project is moved from private to public group. Affected versions are: >=10.2, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.  |
| Git | 2.45.2 | CVE-2020-13353 | ['LOW', 'LOW']       | [2.5, 3.2] | When importing repos via URL, one time use git credentials were persisted beyond the expected time window in Gitaly 1.79.0 or above.   |
| Git | 2.45.2 | CVE-2020-13354 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | A potential DOS vulnerability was discovered in GitLab CE/EE starting with version 12.6. The container registry name check could cause exponential number of backtracks for certain user supplied values resulting in high CPU usage. Affected versions are: >=12.6, <13.3.9.  |
| Git | 2.45.2 | CVE-2020-13358 | ['MEDIUM', 'MEDIUM'] | [4.7, 5.5] | A vulnerability in the internal Kubernetes agent api in GitLab CE/EE version 13.3 and above allows unauthorized access to private projects. Affected versions are: >=13.4, <13.4.5,>=13.3, <13.3.9,>=13.5, <13.5.2.  |
| Git | 2.45.2 | CVE-2020-26406 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Certain SAST CiConfiguration information could be viewed by unauthorized users in GitLab EE starting with 13.3. This information was exposed through GraphQL to non-members of public projects with repository visibility restricted as well as guest members on private projects. Affected versions are: >=13.3, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2020-13350 | ['LOW', 'MEDIUM']    | [3.1, 4.3] | CSRF in runner administration page in all versions of GitLab CE/EE allows an attacker who's able to target GitLab instance administrators to pause/resume runners. Affected versions are >=13.5.0, <13.5.2,>=13.4.0, <13.4.5,<13.3.9.   |
| Git | 2.45.2 | CVE-2020-13351 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Insufficient permission checks in scheduled pipeline API in GitLab CE/EE 13.0+ allows an attacker to read variable names and values for scheduled pipelines on projects visible to the attacker. Affected versions are >=13.0, <13.3.9,>=13.4.0, <13.4.5,>=13.5.0, <13.5.2.                           |
| Git | 2.45.2 | CVE-2020-13348 | ['MEDIUM', 'MEDIUM'] | [5.7, 5.7] | An issue has been discovered in GitLab EE affecting all versions starting from 10.2. Required CODEOWNERS approval could be bypassed by targeting a branch without the CODEOWNERS file. Affected versions are >=10.2, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.   |
| Git | 2.45.2 | CVE-2020-13349 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab EE affecting all versions starting from 8.12. A regular expression related to a file path resulted in the Advanced Search feature susceptible to catastrophic backtracking. Affected versions are >=8.12, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.             |
| Git | 2.45.2 | CVE-2020-26405 | ['HIGH', 'HIGH']     | [7.1, 7.1] | Path traversal vulnerability in package upload functionality in GitLab CE/EE starting from 12.8 allows an attacker to save packages in arbitrary locations. Affected versions are >=12.8, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.  |
| Git | 2.45.2 | CVE-2020-13355 | ['HIGH', 'HIGH']     | [7.5, 8.1] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.14. A path traversal is found in LFS Upload that allows attacker to overwrite certain specific paths on the server. Affected versions are: >=8.14, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.                       |
| Git | 2.45.2 | CVE-2020-13356 | ['HIGH', 'HIGH']     | [8.2, 8.2] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.8.9. A specially crafted request could bypass Multipart protection and read files in certain specific paths on the server. Affected versions are: >=8.8.9, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.               |
| Git | 2.45.2 | CVE-2020-13359 | ['HIGH', 'HIGH']     | [7.6, 7.6] | The Terraform API in GitLab CE/EE 12.10+ exposed the object storage signed URL on the delete operation allowing a malicious project maintainer to overwrite the Terraform state, bypassing audit and other business controls. Affected versions are >=12.10, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2. |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-28991 | CRITICAL             | 9.8        | Gitea 0.9.99 through 1.12.x before 1.12.6 does not prevent a git protocol path that specifies a TCP port number and also contains newlines (with URL encoding) in ParseRemoteAddr in modules/auth/repo_form.go.  |
| Git | 2.45.2 | CVE-2020-26233 | ['HIGH', 'HIGH']     | [7.3, 7.3] | Git Credential Manager Core (GCM Core) is a secure Git credential helper built on .NET Core that runs on Windows and macOS. In Git Credential Manager Core before version 2.0.289, when recursively cloning a Git repository on Windows with submodules, Git will first clone the top-level repository and then recursively clone all submodules by starting new Git processes from the top-level working directory. If a malicious git.exe executable is present in the top-level repository then this binary will be started by Git Credential Manager Core when attempting to read configuration, and not git.exe as found on the %PATH%. This only affects GCM Core on Windows, not macOS or Linux-based distributions. GCM Core version 2.0.289 contains the fix for this vulnerability, and is available from the project's GitHub releases page. GCM Core 2.0.289 is also bundled in the latest Git for Windows release; version 2.29.2(3). As a workaround, users should avoid recursively cloning untrusted repositories wit... |
| Git | 2.45.2 | CVE-2020-28086 | HIGH                 | 7.5        | pass through 1.7.3 has a possibility of using a password for an unintended resource. For exploitation to occur, the user must do a git pull, decrypt a password, and log into a remote service with the password. If an attacker controls the central Git server or one of the other members' machines, and also controls one of the services already in the password store, they can rename one of the password files in the Git repository to something else: pass doesn't correctly verify that the content of a file matches the filename, so a user might be tricked into decrypting the wrong password and sending that to a service that the attacker controls. NOTE: for environments in which this threat model is of concern, signing commits can be a solution.   |
| Git | 2.45.2 | CVE-2020-26407 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.4] | A XSS vulnerability exists in Gitlab CE/EE from 12.4 before 13.4.7, 13.5 before 13.5.5, and 13.6 before 13.6.2 that allows an attacker to perform cross-site scripting to other users via importing a malicious project  |
| Git | 2.45.2 | CVE-2020-26409 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | A DOS vulnerability exists in Gitlab CE/EE >=10.3, <13.4.7, >=13.5, <13.5.5, >=13.6, <13.6.2 that allows an attacker to trigger uncontrolled resource by bypassing input validation in markdown fields.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-13357 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue was discovered in Gitlab CE/EE versions >= 13.1 to <13.4.7, >= 13.5 to <13.5.5, and >= 13.6 to <13.6.2 allowed an unauthorized user to access the user list corresponding to a feature flag in a project.   |
| Git | 2.45.2 | CVE-2020-26408 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | A limited information disclosure vulnerability exists in Gitlab CE/EE from >= 12.2 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2 that allows an attacker to view limited information in user's private profile  |
| Git | 2.45.2 | CVE-2020-26412 | ['LOW', 'MEDIUM']    | [3.1, 4.3] | Removed group members were able to use the To-Do functionality to retrieve updated information on confidential epics starting in GitLab EE 13.2 before 13.6.2.   |
| Git | 2.45.2 | CVE-2020-26413 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 13.6.2. Information disclosure via GraphQL results in user email being unexpectedly visible.   |
| Git | 2.45.2 | CVE-2020-26415 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Information about the starred projects for private user profiles was exposed via the GraphQL API starting from 12.2 via the REST API. This affects GitLab >=12.2 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2.   |
| Git | 2.45.2 | CVE-2020-26416 | ['MEDIUM', 'MEDIUM'] | [4.0, 4.4] | Information disclosure in Advanced Search component of GitLab EE starting from 8.4 results in exposure of search terms via Rails logs. This affects versions >=8.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2.   |
| Git | 2.45.2 | CVE-2020-26417 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Information disclosure via GraphQL in GitLab CE/EE 13.1 and later exposes private group and project membership. This affects versions >=13.6 to <13.6.2, >=13.5 to <13.5.5, and >=13.1 to <13.4.7.   |
| Git | 2.45.2 | CVE-2020-26411 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | A potential DOS vulnerability was discovered in all versions of Gitlab starting from 13.4.x (>=13.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2). Using a specific query name for a project search can cause statement timeouts that can lead to a potential DOS if abused. |
| Git | 2.45.2 | CVE-2020-35236 | MEDIUM               | 5.3        | The GitLab Webhook Handler in amazee.io Lagoon before 1.12.3 has incorrect access control associated with project deletion.  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2020-35702 | HIGH                 | 7.8        | DCTStream::getChars in DCTStream.cc in Poppler 20.12.1 has a heap-based buffer overflow via a crafted PDF document. NOTE: later reports indicate that this only affects builds from Poppler git clones in late December 2020, not the 20.12.1 release. In this situation, it should NOT be considered a Poppler vulnerability. However, several third-party Open Source projects directly rely on Poppler git clones made at arbitrary times, and therefore the CVE remains useful to users of those projects   |
| Git | 2.45.2 | CVE-2021-21236 | ['MEDIUM', 'MEDIUM'] | [5.7, 5.5] | CairoSVG is a Python (pypi) package. CairoSVG is an SVG converter based on Cairo. In CairoSVG before version 2.5.1, there is a regular expression denial of service (REDoS) vulnerability. When processing SVG files, the python package CairoSVG uses two regular expressions which are vulnerable to Regular Expression Denial of Service (REDoS). If an attacker provides a malicious SVG, it can make cairosVG get stuck processing the file for a very long time. This is fixed in version 2.5.1. See Referenced GitHub advisory for more information. |
| Git | 2.45.2 | CVE-2021-3028  | CRITICAL             | 9.8        | git-big-picture before 1.0.0 mishandles ' characters in a branch name, leading to code execution.   |
| Git | 2.45.2 | CVE-2020-26414 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | An issue has been discovered in GitLab affecting all versions starting from 12.4. The regex used for package names is written in a way that makes execution time have quadratic growth based on the length of the malicious input string.   |
| Git | 2.45.2 | CVE-2021-22166 | ['MEDIUM', 'HIGH']   | [5.3, 7.5] | An attacker could cause a Prometheus denial of service in GitLab 13.7+ by sending an HTTP request with a malformed method   |
| Git | 2.45.2 | CVE-2021-22167 | ['MEDIUM', 'HIGH']   | [5.3, 7.5] | An issue has been discovered in GitLab affecting all versions starting from 12.1. Incorrect headers in specific project page allows attacker to have a temporary read access to the private repository  |
| Git | 2.45.2 | CVE-2021-22168 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | A regular expression denial of service issue has been discovered in NuGet API affecting all versions of GitLab starting from version 12.8.  |
| Git | 2.45.2 | CVE-2021-22171 | ['HIGH', 'MEDIUM']   | [7.3, 6.5] | Insufficient validation of authentication parameters in GitLab Pages for GitLab 11.5+ allows an attacker to steal a victim's API token if they click on a maliciously crafted link  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-21237 | ['HIGH', 'HIGH']     | [7.2, 7.8] | Git LFS is a command line extension for managing large files with Git. On Windows, if Git LFS operates on a malicious repository with a git.bat or git.exe file in the current directory, that program would be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. This is the result of an incomplete fix for CVE-2020-27955. This issue occurs because on Windows, Go includes (and prefers) the current directory when the name of a command run does not contain a directory separator. Other than avoiding untrusted repositories or using a different operating system, there is no workaround. This is fixed in v2.13.2. |
| Git | 2.45.2 | CVE-2020-28483 | HIGH                 | 7.1        | This affects all versions of package <a href="https://github.com/gin-gonic/gin">github.com/gin-gonic/gin</a> . When gin is exposed directly to the internet, a client's IP can be spoofed by setting the X-Forwarded-For header.   |
| Git | 2.45.2 | CVE-2021-21253 | ['MEDIUM', 'MEDIUM'] | [5.8, 5.3] | OnlineVotingSystem is an open source project hosted on GitHub. OnlineVotingSystem before version 1.1.2 hashes user passwords without a salt, which is vulnerable to dictionary attacks. Therefore there is a threat of security breach in the voting system. Without a salt, it is much easier for attackers to pre-compute the hash value using dictionary attack techniques such as rainbow tables to crack passwords. This problem is fixed and published in version 1.1.2. A long randomly generated salt is added to the password hash function to better protect passwords stored in the voting system.  |
| Git | 2.45.2 | CVE-2021-3190  | CRITICAL             | 9.8        | The async-git package before 1.13.2 for Node.js allows OS Command Injection via shell metacharacters, as demonstrated by git.reset and git.tag.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-21291 | ['MEDIUM', 'MEDIUM'] | [4.7, 6.1] | OAuth2 Proxy is an open-source reverse proxy and static file server that provides authentication using Providers (Google, GitHub, and others) to validate accounts by email, domain or group. In OAuth2 Proxy before version 7.0.0, for users that use the whitelist domain feature, a domain that ended in a similar way to the intended domain could have been allowed as a redirect. For example, if a whitelist domain was configured for ".example.com", the intention is that subdomains of example.com are allowed. Instead, "example.com" and "badexample.com" could also match. This is fixed in version 7.0.0 onwards. As a workaround, one can disable the whitelist domain feature and run separate OAuth2 Proxy instances for each subdomain.   |
| Git | 2.45.2 | CVE-2021-21293 | ['HIGH', 'HIGH']     | [7.5, 7.5] | blaze is a Scala library for building asynchronous pipelines, with a focus on network IO. All servers running blaze-core before version 0.14.15 are affected by a vulnerability in which unbounded connection acceptance leads to file handle exhaustion. Blaze, accepts connections unconditionally on a dedicated thread pool. This has the net effect of amplifying degradation in services that are unable to handle their current request load, since incoming connections are still accepted and added to an unbounded queue. Each connection allocates a socket handle, which drains a scarce OS resource. This can also confound higher level circuit breakers which work based on detecting failed connections. The vast majority of affected users are using it as part of http4s-blaze-server <= 0.21.16. http4s provides a mechanism for limiting open connections, but is enforced inside the Blaze accept loop, after the connection is accepted and the socket opened. Thus, the limit only prevents the number of con... |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-21294 | ['HIGH', 'HIGH']         | [7.5, 7.5] | Http4s (http4s-blaze-server) is a minimal, idiomatic Scala interface for HTTP services. Http4s before versions 0.21.17, 0.22.0-M2, and 1.0.0-M14 have a vulnerability which can lead to a denial-of-service. Blaze-core, a library underlying http4s-blaze-server, accepts connections unboundedly on its selector pool. This has the net effect of amplifying degradation in services that are unable to handle their current request load, since incoming connections are still accepted and added to an unbounded queue. Each connection allocates a socket handle, which drains a scarce OS resource. This can also confound higher level circuit breakers which work based on detecting failed connections. http4s provides a general "MaxActiveRequests" middleware mechanism for limiting open connections, but it is enforced inside the Blaze accept loop, after the connection is accepted and the socket opened. Thus, the limit only prevents the number of connections which can be simultaneously processed, not the nu... |
| Git | 2.45.2 | CVE-2021-25774 | MEDIUM                   | 4.3        | In JetBrains TeamCity before 2020.2.1, a user could get access to the GitHub access token of another user.   |
| Git | 2.45.2 | CVE-2021-3382  | HIGH                     | 7.5        | Stack buffer overflow vulnerability in gitea 1.9.0 through 1.13.1 allows remote attackers to cause a denial of service (crash) via vectors related to a file path.   |
| Git | 2.45.2 | CVE-2021-26541 | CRITICAL                 | 9.8        | The gitlog function in src/index.ts in gitlog before 4.0.4 has a command injection vulnerability.  |
| Git | 2.45.2 | CVE-2021-22553 | ['MEDIUM', 'HIGH']       | [6.5, 7.5] | Any git operation is passed through Jetty and a session is created. No expiry is set for the session and Jetty does not automatically dispose of the session. Over multiple git actions, this can lead to a heap memory exhaustion for Gerrit servers. We recommend upgrading Gerrit to any of the versions listed above.  |
| Git | 2.45.2 | CVE-2020-28490 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.8] | The package async-git before 1.13.2 are vulnerable to Command Injection via shell meta-characters (back-ticks). For example: git.reset('atouch HACKEDb')   |
| Git | 2.45.2 | CVE-2021-23345 | ['MEDIUM', 'MEDIUM']     | [5.3, 5.3] | All versions of package github.com/thecodingmachine/gotenberg are vulnerable to Server-side Request Forgery (SSRF) via the /convert/html endpoint when the src attribute of an HTML element refers to an internal system file, such as <iframe src='file:///etc/passwd'>.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22187 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting all versions of Gitlab EE/CE before 13.6.7. A potential resource exhaustion issue that allowed running or pending jobs to continue even after project was deleted.  |
| Git | 2.45.2 | CVE-2020-10519 | HIGH                 | 8.8        | A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22.7 and was fixed in 2.22.7, 2.21.15, and 2.20.24. The underlying issues contributing to this vulnerability were identified through the GitHub Security Bug Bounty program.                                       |
| Git | 2.45.2 | CVE-2021-22861 | MEDIUM               | 6.5        | An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to gain write access to unauthorized repositories via specifically crafted pull requests and REST API requests. An attacker would need to be able to fork the targeted repository, a setting that is disabled by default for organization owned private repositories. Branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.4.21 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program. |
| Git | 2.45.2 | CVE-2021-22862 | MEDIUM               | 6.5        | An improper access control vulnerability was identified in GitHub Enterprise Server that allowed an authenticated user with the ability to fork a repository to disclose Actions secrets for the parent repository of the fork. This vulnerability existed due to a flaw that allowed the base reference of a pull request to be updated to point to an arbitrary SHA or another pull request outside of the fork repository. By establishing this incorrect reference in a PR, the restrictions that limit the Actions secrets sent a workflow from forks could be bypassed. This vulnerability affected GitHub Enterprise Server version 3.0.0, 3.0.0.rc2, and 3.0.0.rc1. This vulnerability was reported via the GitHub Bug Bounty program.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22863 | HIGH                 | 8.1        | An improper access control vulnerability was identified in the GitHub Enterprise Server GraphQL API that allowed authenticated users of the instance to modify the maintainer collaboration permission of a pull request without proper authorization. By exploiting this vulnerability, an attacker would be able to gain access to head branches of pull requests opened on repositories of which they are a maintainer. Forking is disabled by default for organization owned private repositories and would prevent this vulnerability. Additionally, branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.12.22 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program. |
| Git | 2.45.2 | CVE-2021-23347 | ['MEDIUM', 'MEDIUM'] | [4.7, 4.8] | The package github.com/argoproj/argo-cd/cmd before 1.7.13, from 1.8.0 and before 1.8.6 are vulnerable to Cross-site Scripting (XSS) the SSO provider connected to Argo CD would have to send back a malicious error message containing JavaScript to the user.   |
| Git | 2.45.2 | CVE-2021-22182 | ['LOW', 'MEDIUM']    | [3.5, 5.4] | An issue has been discovered in GitLab affecting all versions starting with 13.7. GitLab was vulnerable to a stored XSS in merge request.  |
| Git | 2.45.2 | CVE-2021-22188 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab affecting all versions starting with 13.0. Confidential issue titles in Gitlab were readable by an unauthorised user via branch logs.   |
| Git | 2.45.2 | CVE-2021-22183 | ['MEDIUM', 'MEDIUM'] | [4.1, 5.4] | An issue has been discovered in GitLab affecting all versions starting with 11.8. GitLab was vulnerable to a stored XSS in the epics page, which could be exploited with user interactions.  |
| Git | 2.45.2 | CVE-2021-22189 | ['MEDIUM', 'HIGH']   | [5.9, 7.2] | Starting with version 13.7 the Gitlab CE/EE editions were affected by a security issue related to the validation of the certificates for the Fortinet OTP that could result in authentication issues.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-28466 | ['HIGH', 'HIGH']     | [7.5, 7.5] | This affects all versions of package <a href="https://github.com/nats-io/nats-server/server">github.com/nats-io/nats-server/server</a> . 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.  |
| Git | 2.45.2 | CVE-2021-23351 | ['MEDIUM', 'MEDIUM'] | [4.4, 4.9] | The package <a href="https://github.com/pires/go-proxyproto">github.com/pires/go-proxyproto</a> before 0.5.0 are vulnerable to Denial of Service (DoS) via the <code>parseVersion1()</code> function. The reader in this package is a default <code>bufio.Reader</code> wrapping a <code>net.Conn</code> . 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 <code>PROXY</code> 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.   |
| Git | 2.45.2 | CVE-2021-21295 | ['MEDIUM', 'MEDIUM'] | [5.9, 5.9] | Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty ( <code>io.netty:netty-codec-http2</code> ) 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 <code>Http2MultiplexHandler</code> 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 ( <code>HttpRequest</code> , <code>HttpContent</code> , etc.) via <code>Http2StreamFrameToHttpObjectCodec</code> 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 Conte... |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2021-21300 | ['HIGH', 'HIGH']   | [8.0, 7.5] | <p>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 <code>`git config --global core.symlinks false`</code>), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. <code>_before_</code> cloning), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14....</p> |
| Git | 2.45.2 | CVE-2021-21363 | ['MEDIUM', 'HIGH'] | [5.3, 7.0] | <p>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 <code>`outputFolder`</code> 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.</p>   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2021-21368 | ['MEDIUM', 'HIGH'] | [6.7, 8.8] | 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__.<br>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 "pro... |
| Git | 2.45.2 | CVE-2021-28373 | HIGH               | 7.5        | 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.  |
| Git | 2.45.2 | CVE-2021-28378 | ['LOW', 'MEDIUM']  | [3.7, 5.4] | Gitea 1.12.x and 1.13.x before 1.13.4 allows XSS via certain issue data in some situations.   |
| Git | 2.45.2 | CVE-2021-23357 | ['LOW', 'MEDIUM']  | [3.3, 5.3] | All versions of package github.com/tyktechnologies/tyk/gateway are vulnerable to Directory Traversal via the handleAddOrUpdateApi function. This function is able to delete arbitrary JSON files on the disk where Tyk is running via the management API. The APIID is provided by the user and this value is then used to create a file on disk. If there is a file found with the same name then it will be deleted and then re-created with the contents of the API creation request.  |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2021-3344  | HIGH               | 8.8        | A privilege escalation flaw was found in OpenShift builder. During build time, credentials outside the build context are automatically mounted into the container image under construction. An OpenShift user, able to execute code during build time inside this container can re-use the credentials to overwrite arbitrary container images in internal registries and/or escalate their privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This affects <a href="https://github.com/openshift/builder">github.com/openshift/builder</a> v0.0.0-20210125201112-7901cb396121 and before.   |
| Git | 2.45.2 | CVE-2021-21383 | ['HIGH', 'MEDIUM'] | [7.6, 5.4] | Wiki.js an open-source wiki app built on Node.js. Wiki.js before version 2.5.191 is vulnerable to stored cross-site scripting through mustache expressions in code blocks. This vulnerability exists due to mustache expressions being parsed by Vue during content injection even though it is contained within a ` <pre>` element. By creating a crafted wiki page, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the page is viewed by other users. For an example see referenced GitHub Security Advisory. Commit <a href="https://github.com/wikijs/wiki.js/commit/5ffa189383dd716f12b56b8cae2ba0d075996cf1">5ffa189383dd716f12b56b8cae2ba0d075996cf1</a> fixes this vulnerability by adding the v-pre directive to all `<pre>` tags during the render.</pre></pre> |
| Git | 2.45.2 | CVE-2021-21384 | ['MEDIUM', 'HIGH'] | [6.3, 7.8] | shescape is a simple shell escape package for JavaScript. In shescape before version 1.1.3, anyone using <code>_Shescape_</code> to defend against shell injection may still be vulnerable against shell injection if the attacker manages to insert a into the payload. For an example see the referenced GitHub Security Advisory. The problem has been patched in version 1.1.3. No further changes are required.  |
| Git | 2.45.2 | CVE-2021-26275 | CRITICAL           | 9.8        | The eslint-fixer package through 0.1.5 for Node.js allows command injection via shell metacharacters to the fix function. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The ozum/eslint-fixer GitHub repository has been intentionally deleted   |
| Git | 2.45.2 | CVE-2021-28955 | CRITICAL           | 9.8        | git-bug before 0.7.2 has an Uncontrolled Search Path Element. It will execute git.bat from the current directory in certain PATH situations (most often seen on Windows).   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-21401 | ['HIGH', 'HIGH']     | [7.1, 7.1] | Nanopb is a small code-size Protocol Buffers implementation in ansi C. In Nanopb before versions 0.3.9.8 and 0.4.5, decoding a specifically formed message can cause invalid <code>`free()`</code> or <code>`realloc()`</code> calls if the message type contains an <code>`oneof`</code> field, and the <code>`oneof`</code> directly contains both a pointer field and a non-pointer field. If the message data first contains the non-pointer field and then the pointer field, the data of the non-pointer field is incorrectly treated as if it was a pointer value. Such message data rarely occurs in normal messages, but it is a concern when untrusted data is parsed. This has been fixed in versions 0.3.9.8 and 0.4.5. See referenced GitHub Security Advisory for more information including workarounds. |
| Git | 2.45.2 | CVE-2021-22864 | HIGH                 | 8.8        | A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to override environment variables leading to code execution on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.3 and was fixed in 3.0.3, 2.22.9, and 2.21.17. This vulnerability was reported via the GitHub Bug Bounty program.   |
| Git | 2.45.2 | CVE-2021-22176 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting all versions starting with 3.0.1. Improper access control allows demoted project members to access details on authored merge requests  |
| Git | 2.45.2 | CVE-2021-22178 | ['MEDIUM', 'MEDIUM'] | [5.0, 5.0] | An issue has been discovered in GitLab affecting all versions starting from 13.2. Gitlab was vulnerable to SRRF attack through the Prometheus integration.  |
| Git | 2.45.2 | CVE-2021-22179 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | A vulnerability was discovered in GitLab versions before 12.2. GitLab was vulnerable to a SSRF attack through the Outbound Requests feature.  |
| Git | 2.45.2 | CVE-2021-22185 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | Insufficient input sanitization in wikis in GitLab version 13.8 and up allows an attacker to exploit a stored cross-site scripting vulnerability via a specially-crafted commit to a wiki   |
| Git | 2.45.2 | CVE-2021-22186 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | An authorization issue in GitLab CE/EE version 9.4 and up allowed a group maintainer to modify group CI/CD variables which should be restricted to group owners   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-22192 | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.2 allowing unauthorized authenticated users to execute arbitrary code on the server.   |
| Git | 2.45.2 | CVE-2021-22193 | ['LOW', 'LOW']       | [3.5, 3.5] | An issue has been discovered in GitLab affecting all versions starting with 7.1. A member of a private group was able to validate the use of a specific name for private project.   |
| Git | 2.45.2 | CVE-2021-22169 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue was identified in GitLab EE 13.4 or later which leaked internal IP address via error messages.   |
| Git | 2.45.2 | CVE-2021-21403 | ['HIGH', 'CRITICAL'] | [7.5, 9.8] | In github.com/kongchuanhujiao/server before version 1.3.21 there is an authentication Bypass by Primary Weakness vulnerability. All users are impacted. This is fixed in version 1.3.21.  |
| Git | 2.45.2 | CVE-2021-22172 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper authorization in GitLab 12.8+ allows a guest user in a private project to view tag data that should be inaccessible on the releases page   |
| Git | 2.45.2 | CVE-2021-22180 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting all versions starting from 13.4. Improper access control allows unauthorized users to access details on analytic pages.  |
| Git | 2.45.2 | CVE-2021-22184 | ['MEDIUM', 'MEDIUM'] | [6.2, 5.5] | An information disclosure issue in GitLab starting from version 12.8 allowed a user with access to the server logs to see sensitive information that wasn't properly redacted.  |
| Git | 2.45.2 | CVE-2021-22194 | ['MEDIUM', 'MEDIUM'] | [5.7, 4.4] | In all versions of GitLab, marshalled session keys were being stored in Redis.  |
| Git | 2.45.2 | CVE-2021-21411 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | OAuth2-Proxy is an open source reverse proxy that provides authentication with Google, Github or other providers. The `--gitlab-group` flag for group-based authorization in the GitLab provider stopped working in the v7.0.0 release. Regardless of the flag settings, authorization wasn't restricted. Additionally, any authenticated users had whichever groups were set in `--gitlab-group` added to the new `X-Forwarded-Groups` header to the upstream application. While adding GitLab project based authorization support in #630, a bug was introduced where the user session's groups field was populated with the `--gitlab-group` config entries instead of pulling the individual user's group membership from the GitLab Userinfo endpoint. When the session groups were compared against the allowed groups for authorization, they matched improperly (since both lists were populated with the same data) so authorization was allowed. This impacts GitLab Provider users who relies on group membership for aut... |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-29417 | CRITICAL               | 9.8        | gitjacker before 0.1.0 allows remote attackers to execute arbitrary code via a crafted .git directory because of directory traversal.  |
| Git | 2.45.2 | CVE-2021-29642 | MEDIUM                 | 5.3        | GistPad before 0.2.7 allows a crafted workspace folder to change the URL for the Gist API, which leads to leakage of GitHub access tokens.   |
| Git | 2.45.2 | CVE-2021-22177 | ['MEDIUM', 'MEDIUM']   | [4.3, 4.3] | Potential DoS was identified in gitlab-shell in GitLab CE/EE version 12.6.0 or above, which allows an attacker to spike the server resource utilization via gitlab-shell command.  |
| Git | 2.45.2 | CVE-2021-22195 | ['HIGH', 'HIGH']       | [8.6, 7.8] | Client side code execution in gitlab-vscode-extension v3.15.0 and earlier allows attacker to execute code on user system   |
| Git | 2.45.2 | CVE-2021-22196 | ['MEDIUM', 'MEDIUM']   | [6.3, 5.4] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4. It was possible to exploit a stored cross-site-scripting in merge request via a specifically crafted branch name.  |
| Git | 2.45.2 | CVE-2021-22197 | ['LOW', 'MEDIUM']      | [3.5, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.6 where an infinite loop exist when an authenticated user with specific rights access a MR having source and target branch pointing to each other   |
| Git | 2.45.2 | CVE-2021-22198 | ['MEDIUM', 'MEDIUM']   | [4.3, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions from 13.8 and above allowing an authenticated user to delete incident metric images of public projects.  |
| Git | 2.45.2 | CVE-2021-22200 | ['MEDIUM', 'HIGH']     | [5.9, 7.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.6. Under a special condition it was possible to access data of an internal repository through a public project fork as an anonymous user.   |
| Git | 2.45.2 | CVE-2021-22201 | ['CRITICAL', 'MEDIUM'] | [9.6, 6.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.9. A specially crafted import file could read files on the server.  |
| Git | 2.45.2 | CVE-2021-22202 | ['LOW', 'MEDIUM']      | [2.4, 4.3] | An issue has been discovered in GitLab CE/EE affecting all previous versions. If the victim is an admin, it was possible to issue a CSRF in System hooks through the API.  |
| Git | 2.45.2 | CVE-2021-22203 | ['HIGH', 'CRITICAL']   | [7.5, 9.8] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7.9 before 13.8.7, all versions starting from 13.9 before 13.9.5, and all versions starting from 13.10 before 13.10.1. A specially crafted Wiki page allowed attackers to read arbitrary files on the server. |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22865 | MEDIUM             | 6.5        | An improper access control vulnerability was identified in GitHub Enterprise Server that allowed access tokens generated from a GitHub App's web authentication flow to read private repository metadata via the REST API without having been granted the appropriate permissions. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. The private repository metadata returned would be limited to repositories owned by the user the token identifies. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.4 and was fixed in versions 3.0.4, 2.22.10, 2.21.18. This vulnerability was reported via the GitHub Bug Bounty program.   |
| Git | 2.45.2 | CVE-2021-21423 | ['MEDIUM', 'HIGH'] | [6.8, 8.1] | `projen` is a project generation tool that synthesizes project configuration files such as `package.json`, `tsconfig.json`, `.gitignore`, GitHub Workflows, `eslint`, `jest`, and more, from a well-typed definition written in JavaScript. Users of projen's `NodeProject` project type (including any project type derived from it) include a `.github/workflows/rebuild-bot.yml` workflow that may allow any GitHub user to trigger execution of un-trusted code in the context of the "main" repository (as opposed to that of a fork). In some situations, such untrusted code may potentially be able to commit to the "main" repository. The rebuild-bot workflow is triggered by comments including `@projen rebuild` on pull-request to trigger a re-build of the projen project, and updating the pull request with the updated files. This workflow is triggered by an `issue_comment` event, and thus always executes with a `GITHUB_TOKEN` belonging to the repository into which the pull-request is made (this is in c... |
| Git | 2.45.2 | CVE-2021-21432 | ['HIGH', 'MEDIUM'] | [7.5, 6.5] | Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. An authentication mechanism added in version 0.7.0 enables some malicious user to obtain secrets utilizing the injected credentials within the `~/.netrc` file. Refer to the referenced GitHub Security Advisory for complete details. This is fixed in version 0.7.5.  |
| Git | 2.45.2 | CVE-2021-22190 | ['HIGH', 'MEDIUM'] | [8.5, 6.5] | A path traversal vulnerability via the GitLab Workhorse in all versions of GitLab could result in the leakage of a JWT token   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-21394 | ['MEDIUM', 'MEDIUM'] | [5.3, 6.5] | Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 Synapse is missing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource exhaustion. Note that the groups feature is not part of the Matrix specification and the chosen maximum lengths are arbitrary. Not all clients might abide by them. Refer to referenced GitHub security advisory for additional details including workarounds.                                  |
| Git | 2.45.2 | CVE-2021-21392 | ['MEDIUM', 'MEDIUM'] | [6.3, 6.3] | Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 requests to user provided domains were not restricted to external IP addresses when transitional IPv6 addresses were used. Outbound requests to federation, identity servers, when calculating the key validity for third-party invite events, sending push notifications, and generating URL previews are affected. This could cause Synapse to make requests to internal infrastructure on dual-stack networks. See referenced GitHub security advisory for details and workarounds. |
| Git | 2.45.2 | CVE-2021-21393 | ['MEDIUM', 'MEDIUM'] | [5.3, 6.5] | Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 Synapse is missing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource exhaustion. Note that the groups feature is not part of the Matrix specification and the chosen maximum lengths are arbitrary. Not all clients might abide by them. Refer to referenced GitHub security advisory for additional details including workarounds.                                  |
| Git | 2.45.2 | CVE-2021-21399 | ['CRITICAL', 'HIGH'] | [9.1, 7.5] | Ampache is a web based audio/video streaming application and file manager. Versions prior to 4.4.1 allow unauthenticated access to Ampache using the subsonic API. To successfully make the attack you must use a username that is not part of the site to bypass the auth checks. For more details and workaround guidance see the referenced GitHub security advisory.  |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2021-28470 | ['HIGH', 'HIGH'] | [7.8, 7.8] | Visual Studio Code GitHub Pull Requests and Issues Extension Remote Code Execution Vulnerability   |
| Git | 2.45.2 | CVE-2021-29427 | ['HIGH', 'HIGH'] | [8.0, 7.2] | <p>In Gradle from version 5.1 and before version 7.0 there is a vulnerability which can lead to information disclosure and/or dependency poisoning.</p> <p>Repository content filtering is a security control Gradle introduced to help users specify what repositories are used to resolve specific dependencies. This feature was introduced in the wake of the "A Confusing Dependency" blog post. In some cases, Gradle may ignore content filters and search all repositories for dependencies. This only occurs when repository content filtering is used from within a `pluginManagement` block in a settings file. This may change how dependencies are resolved for Gradle plugins and build scripts. For builds that are vulnerable, there are two risks: 1) Information disclosure: Gradle could make dependency requests to repositories outside your organization and leak internal package identifiers. 2) Dependency poisoning/Dependency confusion: Gradle could download a malicious binary from a repository outside your org...</p> |
| Git | 2.45.2 | CVE-2021-29428 | ['HIGH', 'HIGH'] | [8.8, 7.8] | <p>In Gradle before version 7.0, on Unix-like systems, the system temporary directory can be created with open permissions that allow multiple users to create and delete files within it. Gradle builds could be vulnerable to a local privilege escalation from an attacker quickly deleting and recreating files in the system temporary directory. This vulnerability impacted builds using precompiled script plugins written in Kotlin DSL and tests for Gradle plugins written using ProjectBuilder or TestKit. If you are on Windows or modern versions of macOS, you are not vulnerable. If you are on a Unix-like operating system with the "sticky" bit set on your system temporary directory, you are not vulnerable. The problem has been patched and released with Gradle 7.0. As a workaround, on Unix-like operating systems, ensure that the "sticky" bit is set. This only allows the original user (or root) to delete a file. If you are unable to change the permissions of the system temporary directory, you ca...</p>        |

|     |        |                |                          |              |  |
|-----|--------|----------------|--------------------------|--------------|--|
| Git | 2.45.2 | CVE-2021-29437 | ['HIGH', 'MEDIUM']       | [8.0, 6.8]   | ScratchOAuth2 is an OAuth implementation for Scratch. Any ScratchOAuth2-related data normally accessible and modifiable by a user can be read and modified by a third party. 1. Scratch user visits 3rd party site. 2. 3rd party site asks user for Scratch username. 3. 3rd party site pretends to be user and gets login code from ScratchOAuth2. 4. 3rd party site gives code to user and instructs them to post it on their profile. 5. User posts code on their profile, not knowing it is a ScratchOAuth2 login code. 6. 3rd party site completes login with ScratchOAuth2. 7. 3rd party site has full access to anything the user could do if they directly logged in. See referenced GitHub security advisory for patch notes and workarounds. |
| Git | 2.45.2 | CVE-2021-29449 | ['MEDIUM', 'HIGH']       | [6.3, 7.8]   | Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. Multiple privilege escalation vulnerabilities were discovered in version 5.2.4 of Pi-hole core. See the referenced GitHub security advisory for details.   |
| Git | 2.45.2 | CVE-2021-29448 | ['HIGH', 'HIGH']         | [7.6, 8.8]   | Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. The Stored XSS exists in the Pi-hole Admin portal, which can be exploited by the malicious actor with the network access to DNS server. See the referenced GitHub security advisory for patch details.   |
| Git | 2.45.2 | CVE-2021-29434 | ['MEDIUM', 'MEDIUM']     | [6.1, 4.8]   | Wagtail is a Django content management system. In affected versions of Wagtail, when saving the contents of a rich text field in the admin interface, Wagtail does not apply server-side checks to ensure that link URLs use a valid protocol. A malicious user with access to the admin interface could thus craft a POST request to publish content with `javascript:` URLs containing arbitrary code. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. See referenced GitHub advisory for additional details, including a workaround. Patched versions have been released as Wagtail 2.11.7 (for the LTS 2.11 branch) and Wagtail 2.12.4 (for the current 2.12 branch).                        |
| Git | 2.45.2 | CVE-2021-22199 | ['LOW', 'MEDIUM']        | [3.5, 5.4]   | An issue has been discovered in GitLab affecting all versions starting with 12.9. GitLab was vulnerable to a stored XSS if scoped labels were used.  |
| Git | 2.45.2 | CVE-2021-22205 | ['CRITICAL', 'CRITICAL'] | [10.0, 10.0] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.   |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-23365 | ['MEDIUM', 'CRITICAL'] | [4.8, 9.1] | The package <a href="https://github.com/tyktechnologies/tyk-identity-broker">github.com/tyktechnologies/tyk-identity-broker</a> before 1.1.1 are vulnerable to Authentication Bypass via the Go XML parser which can cause SAML authentication bypass. This is because the XML parser doesn't guarantee integrity in the XML round-trip (encoding/decoding XML data).  |
| Git | 2.45.2 | CVE-2021-31863 | HIGH                   | 7.5        | Insufficient input validation in the Git repository integration of Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows Redmine users to read arbitrary local files accessible by the application server process.   |
| Git | 2.45.2 | CVE-2021-29468 | ['HIGH', 'HIGH']       | [8.8, 8.8] | Cygwin Git is a patch set for the git command line tool for the cygwin environment. A specially crafted repository that contains symbolic links as well as files with backslash characters in the file name may cause just-checked out code to be executed while checking out a repository using Git on Cygwin. The problem will be patched in the Cygwin Git v2.31.1-2 release. At time of writing, the vulnerability is present in the upstream Git source code; any Cygwin user who compiles Git for themselves from upstream sources should manually apply a patch to mitigate the vulnerability. As mitigation users should not clone or pull from repositories from untrusted sources. CVE-2019-1354 was an equivalent vulnerability in Git for Visual Studio. |
| Git | 2.45.2 | CVE-2020-15153 | ['HIGH', 'CRITICAL']   | [8.2, 9.8] | Ampache before version 4.2.2 allows unauthenticated users to perform SQL injection. Refer to the referenced GitHub Security Advisory for details and a workaround. This is fixed in version 4.2.2 and the development branch.  |
| Git | 2.45.2 | CVE-2020-7731  | ['HIGH', 'HIGH']       | [7.5, 7.5] | This affects all versions <0.7.0 of package <a href="https://github.com/russellhaering/gosaml2">github.com/russellhaering/gosaml2</a> . There is a crash on nil-pointer dereference caused by sending malformed XML signatures.  |
| Git | 2.45.2 | CVE-2021-22211 | ['LOW', 'MEDIUM']      | [3.1, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7. GitLab Dependency Proxy, under certain circumstances, can impersonate a user resulting in possibly incorrect access handling.  |
| Git | 2.45.2 | CVE-2021-26543 | HIGH                   | 8.8        | The "gitDiff" function in Wayfair git-parse <=1.0.4 has a command injection vulnerability. Clients of the git-parse library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. The issue has been resolved in version 1.0.5.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22206 | ['MEDIUM', 'MEDIUM'] | [6.8, 4.9] | An issue has been discovered in GitLab affecting all versions starting from 11.6. Pull mirror credentials are exposed that allows other maintainers to be able to view the credentials in plain-text,  |
| Git | 2.45.2 | CVE-2021-22208 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting versions starting with 13.5 up to 13.9.7. Improper permission check could allow the change of timestamp for issue creation or update.   |
| Git | 2.45.2 | CVE-2021-22209 | ['HIGH', 'HIGH']     | [7.5, 7.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.8. GitLab was not properly validating authorisation tokens which resulted in GraphQL mutation being executed.   |
| Git | 2.45.2 | CVE-2021-22210 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.2. When querying the repository branches through API, GitLab was ignoring a query parameter and returning a considerable amount of results.   |
| Git | 2.45.2 | CVE-2021-32074 | HIGH                 | 7.5        | HashiCorp vault-action (aka Vault GitHub Action) before 2.2.0 allows attackers to obtain sensitive information from log files because a multi-line secret was not correctly registered with GitHub Actions for log masking.  |
| Git | 2.45.2 | CVE-2021-31913 | HIGH                 | 7.5        | In JetBrains TeamCity before 2020.2.3, insufficient checks of the redirect_uri were made during GitHub SSO token exchange.   |
| Git | 2.45.2 | CVE-2021-29509 | ['HIGH', 'HIGH']     | [7.5, 7.5] | Puma is a concurrent HTTP 1.1 server for Ruby/Rack applications. The fix for CVE-2019-16770 was incomplete. The original fix only protected existing connections that had already been accepted from having their requests starved by greedy persistent-connections saturating all threads in the same process. However, new connections may still be starved by greedy persistent-connections saturating all threads in all processes in the cluster. A `puma` server which received more concurrent `keep-alive` connections than the server had threads in its threadpool would service only a subset of connections, denying service to the unserved connections. This problem has been fixed in `puma` 4.3.8 and 5.3.1. Setting `queue_requests false` also fixes the issue. This is not advised when using `puma` without a reverse proxy, such as `nginx` or `apache`, because you will open yourself to slow client attacks (e.g. slowloris). The fix is very small and a git patch is available for those using unsupported ... |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22866 | HIGH             | 8.8        | A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more permissions to be granted during a GitHub App's user-authorization web flow than was displayed to the user during approval. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. All permissions being granted would properly be shown during the first authorization, but in certain circumstances, if the user revisits the authorization flow after the GitHub App has configured additional user-level permissions, those additional permissions may not be shown, leading to more permissions being granted than the user potentially intended. This vulnerability affected GitHub Enterprise Server 3.0.x prior to 3.0.7 and 2.22.x prior to 2.22.13. It was fixed in versions 3.0.7 and 2.22.13. This vulnerability was reported via the GitHub Bug Bounty program.                                      |
| Git | 2.45.2 | CVE-2021-32629 | ['HIGH', 'HIGH'] | [7.2, 8.8] | Cranelfit is an open-source code generator maintained by Bytecode Alliance. It translates a target-independent intermediate representation into executable machine code. There is a bug in 0.73 of the Cranelfit x64 backend that can create a scenario that could result in a potential sandbox escape in a Wasm program. This bug was introduced in the new backend on 2020-09-08 and first included in a release on 2020-09-30, but the new backend was not the default prior to 0.73. The recently-released version 0.73 with default settings, and prior versions with an explicit build flag to select the new backend, are vulnerable. The bug in question performs a sign-extend instead of a zero-extend on a value loaded from the stack, under a specific set of circumstances. If those circumstances occur, the bug could allow access to memory addresses upto 2GiB before the start of the Wasm program heap. If the heap bound is larger than 2GiB, then it would be possible to read memory from a computable range ... |

|     |        |                |                          |              |  |
|-----|--------|----------------|--------------------------|--------------|--|
| Git | 2.45.2 | CVE-2021-32638 | ['MEDIUM', 'MEDIUM']     | [4.4, 4.4]   | Github's CodeQL action is provided to run CodeQL-based code scanning on non-GitHub CI/CD systems and requires a GitHub access token to connect to a GitHub repository. The runner and its documentation previously suggested passing the GitHub token as a command-line parameter to the process instead of reading it from a file, standard input, or an environment variable. This approach made the token visible to other processes on the same machine, for example in the output of the `ps` command. If the CI system publicly exposes the output of `ps`, for example by logging the output, then the GitHub access token can be exposed beyond the scope intended. Users of the CodeQL runner on 3rd-party systems, who are passing a GitHub token via the `--github-auth` flag, are affected. This applies to both GitHub.com and GitHub Enterprise users. Users of the CodeQL Action on GitHub Actions are not affected. The `--github-auth` flag is now considered insecure and deprecated. The undocumented `--external-... |
| Git | 2.45.2 | CVE-2020-27847 | CRITICAL                 | 9.8          | A vulnerability exists in the SAML connector of the github.com/dexidp/dex library used to process SAML Signature Validation. This flaw allows an attacker to bypass SAML authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. This flaw affects dex versions before 2.27.0.  |
| Git | 2.45.2 | CVE-2021-32637 | ['CRITICAL', 'CRITICAL'] | [10.0, 10.0] | Authelia is a single sign-on multi-factor portal for web apps. This affects users who are using nginx ngx_http_auth_request_module with Authelia, it allows a malicious individual who crafts a malformed HTTP request to bypass the authentication mechanism. It additionally could theoretically affect other proxy servers, but all of the ones we officially support except nginx do not allow malformed URI paths. The problem is rectified entirely in v4.29.3. As this patch is relatively straightforward we can back port this to any version upon request. Alternatively we are supplying a git patch to 4.25.1 which should be relatively straightforward to apply to any version, the git patches for specific versions can be found in the references. The most relevant workaround is upgrading. You can also add a block which fails requests that contains a malformed URI in the internal location block.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-3538  | CRITICAL             | 9.8        | A flaw was found in github.com/satori/go.uuid in versions from commit 0ef6afb2f6cdd6cdaeee3885a95099c63f18fc8c to d91630c8510268e75203009fe7daf2b8e1d60c45. Due to insecure randomness in the g.rand.Read function the generated UUIDs are predictable for an attacker.  |
| Git | 2.45.2 | CVE-2021-22548 | ['MEDIUM', 'HIGH']   | [6.5, 7.8] | An attacker can change the pointer to untrusted memory to point to trusted memory region which causes copying trusted memory to trusted memory, if the latter is later copied out, it allows for reading of memory regions from the trusted region. It is recommended to update past 0.6.2 or git commit <a href="https://github.com/google/asylo/commit/53ed5d8fd8118ced1466e509606dd2f473707a5c">https://github.com/google/asylo/commit/53ed5d8fd8118ced1466e509606dd2f473707a5c</a> |
| Git | 2.45.2 | CVE-2021-22549 | ['MEDIUM', 'HIGH']   | [6.5, 7.8] | An attacker can modify the address to point to trusted memory to overwrite arbitrary trusted memory. It is recommended to update past 0.6.2 or git commit <a href="https://github.com/google/asylo/commit/53ed5d8fd8118ced1466e509606dd2f473707a5c">https://github.com/google/asylo/commit/53ed5d8fd8118ced1466e509606dd2f473707a5c</a>  |
| Git | 2.45.2 | CVE-2021-22550 | ['MEDIUM', 'HIGH']   | [6.5, 7.8] | An attacker can modify the pointers in enclave memory to overwrite arbitrary memory addresses within the secure enclave. It is recommended to update past 0.6.3 or git commit <a href="https://github.com/google/asylo/commit/a47ef55db2337d29de19c50cd29b0deb2871d31c">https://github.com/google/asylo/commit/a47ef55db2337d29de19c50cd29b0deb2871d31c</a>  |
| Git | 2.45.2 | CVE-2021-22214 | ['MEDIUM', 'HIGH']   | [6.8, 8.6] | When requests to the internal network for webhooks are enabled, a server-side request forgery vulnerability in GitLab CE/EE affecting all versions starting from 10.5 was possible to exploit for an unauthenticated attacker even on a GitLab instance where registration is limited  |
| Git | 2.45.2 | CVE-2021-22215 | ['HIGH', 'LOW']      | [7.5, 2.7] | An information disclosure vulnerability in GitLab EE versions 13.11 and later allowed a project owner to leak information about the members' on-call rotations in other projects   |
| Git | 2.45.2 | CVE-2021-22218 | ['LOW', 'LOW']       | [2.6, 2.6] | All versions of GitLab CE/EE starting from 12.8 before 13.10.5, all versions starting from 13.11 before 13.11.5, and all versions starting from 13.12 before 13.12.2 were affected by an issue in the handling of x509 certificates that could be used to spoof author of signed commits.  |
| Git | 2.45.2 | CVE-2021-32673 | ['HIGH', 'CRITICAL'] | [8.8, 9.8] | reg-keygen-git-hash-plugin is a reg-suit plugin to detect the snapshot key to be compare with using Git commit hash. reg-keygen-git-hash-plugin through and including 0.10.15 allow remote attackers to execute of arbitrary commands. Upgrade to version 0.10.16 or later to resolve this issue.  |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22213 | ['HIGH', 'MEDIUM']     | [8.8, 6.5] | A cross-site leak vulnerability in the OAuth flow of all versions of GitLab CE/EE since 7.10 allowed an attacker to leak an OAuth access token by getting the victim to visit a malicious page with Safari   |
| Git | 2.45.2 | CVE-2021-22217 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | A denial of service vulnerability in all versions of GitLab CE/EE before 13.12.2, 13.11.5 or 13.10.5 allows an attacker to cause uncontrolled resource consumption with a specially crafted issue or merge request   |
| Git | 2.45.2 | CVE-2021-22219 | ['MEDIUM', 'MEDIUM']   | [4.4, 4.9] | All versions of GitLab CE/EE starting from 9.5 before 13.10.5, all versions starting from 13.11 before 13.11.5, and all versions starting from 13.12 before 13.12.2 allow a high privilege user to obtain sensitive information from log files because the sensitive information was not correctly registered for log masking.             |
| Git | 2.45.2 | CVE-2021-22221 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | An issue has been discovered in GitLab affecting all versions starting from 12.9.0 before 13.10.5, all versions starting from 13.11.0 before 13.11.5, all versions starting from 13.12.0 before 13.12.2. Insufficient expired password validation in various operations allow user to maintain limited access after their password expired |
| Git | 2.45.2 | CVE-2021-22216 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | A denial of service vulnerability in all versions of GitLab CE/EE before 13.12.2, 13.11.5 or 13.10.5 allows an attacker to cause uncontrolled resource consumption with a very long issue or merge request description   |
| Git | 2.45.2 | CVE-2021-22220 | ['MEDIUM', 'MEDIUM']   | [6.1, 5.4] | An issue has been discovered in GitLab affecting all versions starting with 13.10. GitLab was vulnerable to a stored XSS in blob viewer of notebooks.  |
| Git | 2.45.2 | CVE-2021-34364 | MEDIUM                 | 6.1        | The Refined GitHub browser extension before 21.6.8 might allow XSS via a link in a document. NOTE: github.com sends Content-Security-Policy headers to, in general, address XSS and other concerns.  |
| Git | 2.45.2 | CVE-2021-22175 | ['MEDIUM', 'CRITICAL'] | [6.8, 9.8] | When requests to the internal network for webhooks are enabled, a server-side request forgery vulnerability in GitLab affecting all versions starting from 10.5 was possible to exploit for an unauthenticated attacker even on a GitLab instance where registration is disabled   |
| Git | 2.45.2 | CVE-2021-22181 | ['HIGH', 'MEDIUM']     | [7.7, 6.5] | A denial of service vulnerability in GitLab CE/EE affecting all versions since 11.8 allows an attacker to create a recursive pipeline relationship and exhaust resources.  |
| Git | 2.45.2 | CVE-2021-35206 | MEDIUM                 | 6.1        | Gitpod before 0.6.0 allows unvalidated redirects.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22226 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Under certain conditions, some users were able to push to protected branches that were restricted to deploy keys in GitLab CE/EE since version 13.9  |
| Git | 2.45.2 | CVE-2021-22229 | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.8. Under a special condition it was possible to access data of an internal repository through project fork done by a project member.  |
| Git | 2.45.2 | CVE-2021-22232 | ['LOW', 'MEDIUM']    | [3.5, 5.4] | HTML injection was possible via the full name field before versions 13.11.6, 13.12.6, and 14.0.2 in GitLab CE  |
| Git | 2.45.2 | CVE-2021-22223 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | Client-Side code injection through Feature Flag name in GitLab CE/EE starting with 11.9 allows a specially crafted feature flag name to PUT requests on behalf of other users via clicking on a link   |
| Git | 2.45.2 | CVE-2021-22228 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An issue has been discovered in GitLab affecting all versions before 13.11.6, all versions starting from 13.12 before 13.12.6, and all versions starting from 14.0 before 14.0.2. Improper access control allows unauthorised users to access project details using GraphQL. |
| Git | 2.45.2 | CVE-2021-22227 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | A reflected cross-site script vulnerability in GitLab before versions 13.11.6, 13.12.6 and 14.0.2 allowed an attacker to send a malicious link to a victim and trigger actions on their behalf if they clicked it  |
| Git | 2.45.2 | CVE-2021-22230 | ['MEDIUM', 'HIGH']   | [4.9, 7.2] | Improper code rendering while rendering merge requests could be exploited to submit malicious code. This vulnerability affects GitLab CE/EE 9.3 and later through 13.11.6, 13.12.6, and 14.0.2.  |
| Git | 2.45.2 | CVE-2021-22231 | ['LOW', 'MEDIUM']    | [3.5, 4.3] | A denial of service in user's profile page is found starting with GitLab CE/EE 8.0 that allows attacker to reject access to their profile page via using a specially crafted username.   |
| Git | 2.45.2 | CVE-2021-22224 | ['HIGH', 'MEDIUM']   | [7.1, 6.5] | A cross-site request forgery vulnerability in the GraphQL API in GitLab since version 13.12 and before versions 13.12.6 and 14.0.2 allowed an attacker to call mutations as the victim   |
| Git | 2.45.2 | CVE-2021-22225 | ['MEDIUM', 'MEDIUM'] | [4.7, 5.4] | Insufficient input sanitization in markdown in GitLab version 13.11 and up allows an attacker to exploit a stored cross-site scripting vulnerability via a specially-crafted markdown  |
| Git | 2.45.2 | CVE-2021-22233 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An information disclosure vulnerability in GitLab EE versions 13.10 and later allowed a user to read project details   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2020-20250 | MEDIUM               | 6.5        | Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). NOTE: this is different from CVE-2020-20253 and CVE-2020-20254. All four vulnerabilities in the /nova/bin/lcdstat process are discussed in the CVE-2020-20250 <a href="https://github.com/cq674350529">github.com/cq674350529</a> reference.  |
| Git | 2.45.2 | CVE-2021-22867 | MEDIUM               | 6.5        | A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.3 and was fixed in 3.1.3, 3.0.11, and 2.22.17. This vulnerability was reported via the GitHub Bug Bounty program. |
| Git | 2.45.2 | CVE-2021-23409 | ['HIGH', 'HIGH']     | [7.5, 7.5] | The package <a href="https://github.com/pires/go-proxyproto">github.com/pires/go-proxyproto</a> before 0.6.0 are vulnerable to Denial of Service (DoS) via creating connections without the proxy protocol header.   |
| Git | 2.45.2 | CVE-2020-22283 | HIGH                 | 7.5        | A buffer overflow vulnerability in the <code>icmp6_send_response_with_addrs_and_netif()</code> function of Free Software Foundation lwIP version git head allows attackers to access sensitive information via a crafted ICMPv6 packet.  |
| Git | 2.45.2 | CVE-2020-22284 | HIGH                 | 7.5        | A buffer overflow vulnerability in the <code>zepif_linkoutput()</code> function of Free Software Foundation lwIP git head version and version 2.1.2 allows attackers to access sensitive information via a crafted 6LoWPAN packet.   |
| Git | 2.45.2 | CVE-2021-23412 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | All versions of package <a href="https://github.com/gitlogplus">gitlogplus</a> are vulnerable to Command Injection via the main functionality, as options attributes are appended to the command to be executed without sanitization.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-32783 | ['HIGH', 'HIGH']     | [8.5, 8.5] | Contour is a Kubernetes ingress controller using Envoy proxy. In Contour before version 1.17.1 a specially crafted ExternalName type Service may be used to access Envoy's admin interface, which Contour normally prevents from access outside the Envoy container. This can be used to shut down Envoy remotely (a denial of service), or to expose the existence of any Secret that Envoy is using for its configuration, including most notably TLS Keypairs. However, it <i>*cannot*</i> be used to get the <i>*content*</i> of those secrets. Since this attack allows access to the administration interface, a variety of administration options are available, such as shutting down the Envoy or draining traffic. In general, the Envoy admin interface cannot easily be used for making changes to the cluster, in-flight requests, or backend services, but it could be used to shut down or drain Envoy, change traffic routing, or to retrieve secret metadata, as mentioned above. The issue will be addressed in Contour v1.18.0 a... |
| Git | 2.45.2 | CVE-2021-32804 | ['HIGH', 'HIGH']     | [8.2, 8.1] | The npm package "tar" (aka node-tar) before versions 6.1.1, 5.0.6, 4.4.14, and 3.3.2 has a arbitrary File Creation/Overwrite vulnerability due to insufficient absolute path sanitization. node-tar aims to prevent extraction of absolute file paths by turning absolute paths into relative paths when the `preservePaths` flag is not set to `true`. This is achieved by stripping the absolute path root from any absolute file paths contained in a tar file. For example `/home/user/.bashrc` would turn into `home/user/.bashrc`. This logic was insufficient when file paths contained repeated path roots such as `///home/user/.bashrc`. `node-tar` would only strip a single path root from such paths. When given an absolute file path with repeating path roots, the resulting path (e.g. `///home/user/.bashrc`) would still resolve to an absolute path, thus allowing arbitrary file creation and overwrite. This issue was addressed in releases 3.2.2, 4.4.14, 5.0.6 and 6.1.1. Users may work around this vulner...                |
| Git | 2.45.2 | CVE-2021-22240 | ['MEDIUM', 'MEDIUM'] | [4.2, 4.3] | Improper access control in GitLab EE versions 13.11.6, 13.12.6, and 14.0.2 allows users to be created via single sign on despite user cap being enabled  |
| Git | 2.45.2 | CVE-2021-22241 | ['HIGH', 'MEDIUM']   | [8.7, 5.4] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.0. It was possible to exploit a stored cross-site-scripting via a specifically crafted default branch name.   |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22234 | ['CRITICAL', 'MEDIUM'] | [9.6, 6.4] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.11 before 13.11.7, all versions starting from 13.12 before 13.12.8, and all versions starting from 14.0 before 14.0.4. A specially crafted design image allowed attackers to read arbitrary files on the server.  |
| Git | 2.45.2 | CVE-2021-38599 | HIGH                   | 7.5        | WAL-G before 1.1, when a non-libsodium build (e.g., one of the official binary releases published as GitHub Releases) is used, silently ignores the libsodium encryption key and uploads cleartext backups. This is arguably a Principle of Least Surprise violation because "the user likely wanted to encrypt all file activity."  |
| Git | 2.45.2 | CVE-2021-37636 | ['MEDIUM', 'MEDIUM']   | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of <code>`tf.raw_ops.SparseDenseCwiseDiv`</code> is vulnerable to a division by 0 error. The [implementation](https://github.com/tensorflow/tensorflow/blob/a1bc56203f21a5a4995311825ffaba7a670d7747/tensorflow/core/kernels/sparse_dense_binary_op_shared.cc#L56) uses a common class for all binary operations but fails to treat the division by 0 case separately. We have patched the issue in GitHub commit d9204be9f49520cdaeb2541d1dc5187b23f31d9. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.   |
| Git | 2.45.2 | CVE-2021-37640 | ['MEDIUM', 'MEDIUM']   | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of <code>`tf.raw_ops.SparseReshape`</code> can be made to trigger an integral division by 0 exception. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/reshape_util.cc#L176-L181) calls the reshaping functor whenever there is at least an index in the input but does not check that shape of the input or the target shape have both a non-zero number of elements. The [reshape functor](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/reshape_util.cc#L40-L78) blindly divides by the dimensions of the target shape. Hence, if this is not checked, code will result in a division by 0. We have patched the issue in GitHub commit 4923de56ec94fff7770df259ab7f2288a74feb41. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on Tensoro... |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37642 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of <code>`tf.raw_ops.ResourceScatterDiv`</code> is vulnerable to a division by 0 error. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/resource_variable_ops.cc#L865) uses a common class for all binary operations but fails to treat the division by 0 case separately. We have patched the issue in GitHub commit 4aacb30888638da75023e6601149415b39763d76. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.   |
| Git | 2.45.2 | CVE-2021-37653 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a crash via a floating point exception in <code>`tf.raw_ops.ResourceGather`</code> . The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/resource_variable_ops.cc#L725-L731) computes the value of a value, <code>`batch_size`</code> , and then divides by it without checking that this value is not 0. We have patched the issue in GitHub commit ac117ee8a8ea57b73d34665cdf00ef3303bc0b11. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.   |
| Git | 2.45.2 | CVE-2021-37660 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause a floating point exception by calling inplace operations with crafted arguments that would result in a division by 0. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/inplace_ops.cc#L283) has a logic error: it should skip processing if <code>`x`</code> and <code>`v`</code> are empty but the code uses <code>`  `</code> instead of <code>`&amp;&amp;`</code> . We have patched the issue in GitHub commit e86605c0a336c088b638da02135ea6f9f6753618. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range. |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37637 | ['HIGH', 'MEDIUM'] | [7.7, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. It is possible to trigger a null pointer dereference in TensorFlow by passing an invalid input to <code>`tf.raw_ops.CompressElement`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/tensorflow/core/data/compression_utils.cc#L34) was accessing the size of a buffer obtained from the return of a separate function call before validating that said buffer is valid. We have patched the issue in GitHub commit 5dc7f6981fdaf74c8c5be41f393df705841fb7c5. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>                                     |
| Git | 2.45.2 | CVE-2021-37638 | ['HIGH', 'HIGH']   | [7.7, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. Sending invalid argument for <code>`row_partition_types`</code> of <code>`tf.raw_ops.RaggedTensorToTensor`</code> API results in a null pointer dereference and undefined behavior. The [implementation](https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc#L328) accesses the first element of a user supplied list of values without validating that the provided list is not empty. We have patched the issue in GitHub commit 301ae88b331d37a2a16159b65b255f4f9eb39314. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37639 | ['HIGH', 'HIGH'] | [8.4, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. When restoring tensors via raw APIs, if the tensor name is not provided, TensorFlow can be tricked into dereferencing a null pointer. Alternatively, attackers can read memory outside the bounds of heap allocated data by providing some tensor names but not enough for a successful restoration. The [implementation](https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/tensorflow/core/kernels/save_restore_tensor.cc#L158-L159) retrieves the tensor list corresponding to the `tensor_name` user controlled input and immediately retrieves the tensor at the restoration index (controlled via `preferred_shard` argument). This occurs without validating that the provided list has enough values. If the list is empty this results in dereferencing a null pointer (undefined behavior). If, however, the list has some elements, if the restoration index is outside the bounds this results in heap OOB rea...</p> |
| Git | 2.45.2 | CVE-2021-37643 | ['HIGH', 'HIGH'] | [7.7, 7.1] | <p>TensorFlow is an end-to-end open source platform for machine learning. If a user does not provide a valid padding value to `tf.raw_ops.MatrixDiagPartOp`, then the code triggers a null pointer dereference (if input is empty) or produces invalid behavior, ignoring all values after the first. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/linalg/matrix_diag_op.cc#L89) reads the first value from a tensor buffer without first checking that the tensor has values to read from. We have patched the issue in GitHub commit 482da92095c4d48f8784b1f00dda4f81c28d2988. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37647 | ['HIGH', 'MEDIUM'] | [7.7, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. When a user does not supply arguments that determine a valid sparse tensor, <code>`tf.raw_ops.SparseTensorSliceDataset`</code> implementation can be made to dereference a null pointer. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/data/sparse_tensor_slice_dataset_op.cc#L240-L251) has some argument validation but fails to consider the case when either <code>`indices`</code> or <code>`values`</code> are provided for an empty sparse tensor when the other is not. If <code>`indices`</code> is empty, then [code that performs validation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/data/sparse_tensor_slice_dataset_op.cc#L260-L261) (i.e., checking that the indices are monotonically increasing) results in a null pointer dereference. If <code>`indices`</code> as provided by the user is empty, then <code>`indices`</code> in the C++ code above is backe...</p> |
| Git | 2.45.2 | CVE-2021-37649 | ['HIGH', 'MEDIUM'] | [7.7, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. The code for <code>`tf.raw_ops.UncompressElement`</code> can be made to trigger a null pointer dereference. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/data/experimental/compression_ops.cc#L50-L53) obtains a pointer to a <code>`CompressedElement`</code> from a <code>`Variant`</code> tensor and then proceeds to dereference it for decompressing. There is no check that the <code>`Variant`</code> tensor contained a <code>`CompressedElement`</code>, so the pointer is actually <code>`nullptr`</code>. We have patched the issue in GitHub commit 7bdf50bb4f5c54a4997c379092888546c97c3ebd. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37635 | ['HIGH', 'HIGH'] | [7.3, 7.1] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of sparse reduction operations in TensorFlow can trigger accesses outside of bounds of heap allocated data. The [implementation](<a href="https://github.com/tensorflow/tensorflow/blob/a1bc56203f21a5a4995311825ffaba7a670d7747/tensorflow/core/kernels/sparse_reduce_op.cc#L217-L228">https://github.com/tensorflow/tensorflow/blob/a1bc56203f21a5a4995311825ffaba7a670d7747/tensorflow/core/kernels/sparse_reduce_op.cc#L217-L228</a>) fails to validate that each reduction group does not overflow and that each corresponding index does not point to outside the bounds of the input tensor. We have patched the issue in GitHub commit 87158f43f05f2720a374f3e6d22a7aaa3a33f750. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |
| Git | 2.45.2 | CVE-2021-37641 | ['HIGH', 'HIGH'] | [7.3, 7.1] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions if the arguments to `tf.raw_ops.RaggedGather` don't determine a valid ragged tensor code can trigger a read from outside of bounds of heap allocated buffers. The [implementation](<a href="https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/ragged_gather_op.cc#L70">https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/ragged_gather_op.cc#L70</a>) directly reads the first dimension of a tensor shape before checking that said tensor has rank of at least 1 (i.e., it is not a scalar). Furthermore, the implementation does not check that the list given by `params_nested_splits` is not an empty list of tensors. We have patched the issue in GitHub commit a2b743f6017d7b97af1fe49087ae15f0ac634373. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37644 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions providing a negative element to `num_elements` list argument of `tf.raw_ops.TensorListReserve` causes the runtime to abort the process due to reallocating a `std::vector` to have a negative number of elements. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/list_kernels.cc#L312) calls `std::vector.resize()` with the new size controlled by input given by the user, without checking that this input is valid. We have patched the issue in GitHub commit 8a6e874437670045e6c7dc6154c7412b4a2135e2. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37645 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of `tf.raw_ops.QuantizeAndDequantizeV4Grad` is vulnerable to an integer overflow issue caused by converting a signed integer value to an unsigned one and then allocating memory based on this value. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/quantize_and_dequantize_op.cc#L126) uses the `axis` value as the size argument to `absl::InlinedVector` constructor. But, the constructor uses an unsigned type for the argument, so the implicit conversion transforms the negative value to a large integer. We have patched the issue in GitHub commit 96f364a1ca3009f98980021c4b32be5fdcca33a1. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, and TensorFlow 2.4.3, as these are also affected and still in supported range.</p> |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37646 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of <code>`tf.raw_ops.StringNGrams`</code> is vulnerable to an integer overflow issue caused by converting a signed integer value to an unsigned one and then allocating memory based on this value. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/string_ngrams_op.cc#L184) calls <code>`reserve`</code> on a <code>`tstring`</code> with a value that sometimes can be negative if user supplies negative <code>`ngram_widths`</code>. The <code>`reserve`</code> method calls <code>`TF_TString_Reserve`</code> which has an <code>`unsigned long`</code> argument for the size of the buffer. Hence, the implicit conversion transforms the negative value to a large integer. We have patched the issue in GitHub commit <a href="https://github.com/tensorflow/tensorflow/commit/c283e542a3f422420cfdb332414543b62fc4e4a5">c283e542a3f422420cfdb332414543b62fc4e4a5</a>. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as th...</p> |
| Git | 2.45.2 | CVE-2021-37650 | ['HIGH', 'HIGH']     | [7.8, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation for <code>`tf.raw_ops.ExperimentalDatasetToTFRecord`</code> and <code>`tf.raw_ops.DatasetToTFRecord`</code> can trigger heap buffer overflow and segmentation fault. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/data/experimental/to_tf_record_op.cc#L93-L102) assumes that all records in the dataset are of string type. However, there is no check for that, and the example given above uses numeric types. We have patched the issue in GitHub commit <a href="https://github.com/tensorflow/tensorflow/commit/e0b6e58c328059829c3eb968136f17aa72b6c876">e0b6e58c328059829c3eb968136f17aa72b6c876</a>. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37651 | ['HIGH', 'HIGH'] | [7.1, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation for <code>`tf.raw_ops.FractionalAvgPoolGrad`</code> can be tricked into accessing data outside of bounds of heap allocated buffers. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/fractional_avg_pool_op.cc#L205) does not validate that the input tensor is non-empty. Thus, code constructs an empty <code>`EigenDoubleMatrixMap`</code> and then accesses this buffer with indices that are outside of the empty area. We have patched the issue in GitHub commit 0f931751fb20f565c4e94aa6df58d54a003cdb30. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |
| Git | 2.45.2 | CVE-2021-37654 | ['HIGH', 'HIGH'] | [7.3, 7.1] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a crash via a <code>`CHECK`</code>-fail in debug builds of TensorFlow using <code>`tf.raw_ops.ResourceGather`</code> or a read from outside the bounds of heap allocated data in the same API in a release build. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernel_s/resource_variable_ops.cc#L660-L668) does not check that the <code>`batch_dims`</code> value that the user supplies is less than the rank of the input tensor. Since the implementation uses several for loops over the dimensions of <code>`tensor`</code>, this results in reading data from outside the bounds of heap allocated buffer backing the tensor. We have patched the issue in GitHub commit bc9c546ce7015c57c2f15c168b3d9201de679a1d. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are ...</p> |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37655 | ['HIGH', 'HIGH'] | [7.3, 7.3] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a read from outside of bounds of heap allocated data by sending invalid arguments to <code>`tf.raw_ops.ResourceScatterUpdate`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/resource_variable_ops.cc#L919-L923) has an incomplete validation of the relationship between the shapes of <code>`indices`</code> and <code>`updates`</code>: instead of checking that the shape of <code>`indices`</code> is a prefix of the shape of <code>`updates`</code> (so that broadcasting can happen), code only checks that the number of elements in these two tensors are in a divisibility relationship. We have patched the issue in GitHub commit 01cff3f986259d661103412a20745928c727326f. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in suppo...</p> |
| Git | 2.45.2 | CVE-2021-37656 | ['HIGH', 'HIGH'] | [7.1, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in <code>`tf.raw_ops.RaggedTensorToSparse`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/ragged_tensor_to_sparse_kernel.cc#L30) has an incomplete validation of the splits values: it does not check that they are in increasing order. We have patched the issue in GitHub commit 1071f554dbd09f7e101324d366eec5f4fe5a3ece. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37657 | ['HIGH', 'HIGH'] | [7.1, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in all operations of type <code>`tf.raw_ops.MatrixDiagV*`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/linalg/matrix_diag_op.cc) has incomplete validation that the value of <code>`k`</code> is a valid tensor. We have check that this value is either a scalar or a vector, but there is no check for the number of elements. If this is an empty tensor, then code that accesses the first element of the tensor is wrong. We have patched the issue in GitHub commit f2a673bd34f0d64b8e40a551ac78989d16daad09. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>    |
| Git | 2.45.2 | CVE-2021-37658 | ['HIGH', 'HIGH'] | [7.1, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in all operations of type <code>`tf.raw_ops.MatrixSetDiagV*`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/linalg/matrix_diag_op.cc) has incomplete validation that the value of <code>`k`</code> is a valid tensor. We have check that this value is either a scalar or a vector, but there is no check for the number of elements. If this is an empty tensor, then code that accesses the first element of the tensor is wrong. We have patched the issue in GitHub commit ff8894044dfae5568ecbf2ed514c1a37dc394f1b. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37659 | ['HIGH', 'HIGH']     | [7.3, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in all binary cwise operations that don't require broadcasting (e.g., gradients of binary cwise operations). The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/cwise_ops_common.h#L264) assumes that the two inputs have exactly the same number of elements but does not check that. Hence, when the eigen functor executes it triggers heap OOB reads and undefined behavior due to binding to nullptr. We have patched the issue in GitHub commit 93f428fd1768df147171ed674fee1fc5ab8309ec. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |
| Git | 2.45.2 | CVE-2021-37661 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause a denial of service in `boosted_trees_create_quantile_stream_resource` by using negative arguments. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/quantile_ops.cc#L96) does not validate that `num_streams` only contains non-negative numbers. In turn, [this results in using this value to allocate memory](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/quantiles/quantile_stream_resource.h#L31-L40). However, `reserve` receives an unsigned integer so there is an implicit conversion from a negative value to a large positive unsigned. This results in a crash from the standard library. We have patched the issue in GitHub commit 8a84f7a2b5a2b27ecf88d25bad9ac777cd2f7992. The fix will be included in TensorFlo...</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37662 | ['HIGH', 'HIGH']     | [7.1, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can generate undefined behavior via a reference binding to nullptr in <code>`BoostedTreesCalculateBestGainsPerFeature`</code> and similar attack can occur in <code>`BoostedTreesCalculateBestFeatureSplitV2`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/stats_ops.cc) does not validate the input values. We have patched the issue in GitHub commit 9c87c32c710d0b5b53dc6fd3bfde4046e1f7a5ad and in commit 429f009d2b2c09028647dd4bb7b3f6f414bbaad7. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |
| Git | 2.45.2 | CVE-2021-37664 | ['HIGH', 'HIGH']     | [7.3, 7.1] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can read from outside of bounds of heap allocated data by sending specially crafted illegal arguments to <code>`BoostedTreesSparseCalculateBestFeatureSplit`</code>. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/stats_ops.cc) needs to validate that each value in <code>`stats_summary_indices`</code> is in range. We have patched the issue in GitHub commit e84c975313e8e8e38bb2ea118196369c45c51378. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37700 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.1] | <p>@github/paste-markdown is an npm package for pasting markdown objects. A self Cross-Site Scripting vulnerability exists in the @github/paste-markdown before version 0.3.4. If the clipboard data contains the string <code>`&lt;table&gt;`</code>, a <code>**div**</code> is dynamically created, and the clipboard content is copied into its <code>**innerHTML**</code> property without any sanitization, resulting in improper execution of JavaScript in the browser of the victim (the user who pasted the code). Users directed to copy text from a malicious website and paste it into pages that utilize this library are affected. This is fixed in version 0.3.4. Refer the to the referenced GitHub Advisory for more details including an example exploit.</p>   |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37648 | ['HIGH', 'HIGH'] | [7.8, 7.8] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions the code for <code>`tf.raw_ops.SaveV2`</code> does not properly validate the inputs and an attacker can trigger a null pointer dereference. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/save_restore_v2_ops.cc) uses <code>`ValidateInputs`</code> to check that the input arguments are valid. This validation would have caught the illegal state represented by the reproducer above. However, the validation uses <code>`OP_REQUIRES`</code> which translates to setting the <code>`Status`</code> object of the current <code>`OpKernelContext`</code> to an error status, followed by an empty <code>`return`</code> statement which just terminates the execution of the function it is present in. However, this does not mean that the kernel execution is finalized: instead, execution continues from the next line in <code>`Compute`</code> that follows the call to <code>`ValidateInputs`</code> . This is equivalent to lacking the valida... |
| Git | 2.45.2 | CVE-2021-37652 | ['HIGH', 'HIGH'] | [7.8, 7.8] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation for <code>`tf.raw_ops.BoostedTreesCreateEnsemble`</code> can result in a use after free error if an attacker supplies specially crafted arguments. The [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/boosted_trees/resource_ops.cc#L55) uses a reference counted resource and decrements the refcount if the initialization fails, as it should. However, when the code was written, the resource was represented as a naked pointer but later refactoring has changed it to be a smart pointer. Thus, when the pointer leaves the scope, a subsequent <code>`free`</code> -ing of the resource occurs, but this fails to take into account that the refcount has already reached 0, thus the resource has been already freed. During this double-free process, members of the resource object are accessed for cleanup but they are invalid as the entire reso...   |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37666 | ['HIGH', 'HIGH'] | [7.8, 7.8] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in <code>`tf.raw_ops.RaggedTensorToVariant`</code> . The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/ragged_tensor_to_variant_op.cc#L129) has an incomplete validation of the splits values, missing the case when the argument would be empty. We have patched the issue in GitHub commit be7a4de6adfb303ce08be4332554d ff70362612. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.  |
| Git | 2.45.2 | CVE-2021-37667 | ['HIGH', 'HIGH'] | [7.8, 7.8] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in <code>`tf.raw_ops.UnicodeEncode`</code> . The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/unicode_ops.cc#L533-L539) reads the first dimension of the <code>`input_splits`</code> tensor before validating that this tensor is not empty. We have patched the issue in GitHub commit 2e0ee46f1a47675152d3d865797a18358881d7a6. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.  |
| Git | 2.45.2 | CVE-2021-37671 | ['HIGH', 'HIGH'] | [7.8, 7.8] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in <code>`tf.raw_ops.Map*`</code> and <code>`tf.raw_ops.OrderedMap*`</code> operations. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/map_stage_op.cc#L222-L248) has a check in place to ensure that <code>`indices`</code> is in ascending order, but does not check that <code>`indices`</code> is not empty. We have patched the issue in GitHub commit 532f5c5a547126c634fed43bbad1dc6417678ac. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range. |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37675 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions most implementations of convolution operators in TensorFlow are affected by a division by 0 vulnerability where an attacker can trigger a denial of service via a crash. The shape inference [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/framework/common_shape_fns.cc#L577) is missing several validations before doing divisions and modulo operations. We have patched the issue in GitHub commit 8a793b5d7f59e37ac7f3cd0954a750a2fe76bad4. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range. |
| Git | 2.45.2 | CVE-2021-37676 | ['HIGH', 'HIGH']     | [7.8, 7.8] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in `tf.raw_ops.SparseFillEmptyRows`. The shape inference [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/ops/sparse_ops.cc#L608-L634) does not validate that the input arguments are not empty tensors. We have patched the issue in GitHub commit 578e634b4f1c1c684d4b4294f9e5281b2133b3ed. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.  |
| Git | 2.45.2 | CVE-2021-37680 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of fully connected layers in TFLite is [vulnerable to a division by zero error](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/fully_connected.cc#L226). We have patched the issue in GitHub commit 718721986aa137691ee23f03638867151f74935f. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37681 | ['HIGH', 'HIGH']     | [7.8, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of SVDF in TFLite is [vulnerable to a null pointer error](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/svdf.cc#L300-L313). The [ `GetVariableInput` function](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/kernel_util.cc#L115-L119) can return a null pointer but `GetTensorData` assumes that the argument is always a valid tensor. Furthermore, because `GetVariableInput` calls [ `GetMutableInput` ](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/kernel_util.cc#L82-L90) which might return `nullptr`, the `tensor-&gt;is_variable` expression can also trigger a null pointer exception. We have patched the issue in GitHub commit 5b048e87e4e55990dae6b547add4dae59f4e1c76. The fix will be included in Tens...</p> |
| Git | 2.45.2 | CVE-2021-37686 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the strided slice implementation in TFLite has a logic bug which can allow an attacker to trigger an infinite loop. This arises from newly introduced support for [ellipsis in axis definition](https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/strided_slice.cc#L103-L122). An attacker can craft a model such that `ellipsis_end_idx` is smaller than `i` (e.g., always negative). In this case, the inner loop does not increase `i` and the `continue` statement causes execution to skip over the preincrement at the end of the outer loop. We have patched the issue in GitHub commit dfa22b348b70bb89d6d6ec0ff53973bacb4f4695. TensorFlow 2.6.0 is the only affected version.</p>   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37688 | ['HIGH', 'MEDIUM'] | [7.8, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can craft a TFLite model that would trigger a null pointer dereference, which would result in a crash and denial of service. The [implementation](https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/internal/optimized/optimized_ops.h#L268-L285) unconditionally dereferences a pointer. We have patched the issue in GitHub commit 15691e456c7dc9bd6be203b09765b063bf4a380c. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |
| Git | 2.45.2 | CVE-2021-37689 | ['HIGH', 'MEDIUM'] | [7.8, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can craft a TFLite model that would trigger a null pointer dereference, which would result in a crash and denial of service. This is caused by the MLIR optimization of `L2NormalizeReduceAxis` operator. The [implementation](https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/compiler/mlir/lite/transforms/optimize.cc#L67-L70) unconditionally dereferences a pointer to an iterator to a vector without checking that the vector has elements. We have patched the issue in GitHub commit d6b57f461b39fd1aa8c1b870f1b974aac3554955. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37663 | ['HIGH', 'HIGH'] | [7.8, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions due to incomplete validation in `tf.raw_ops.QuantizeV2`, an attacker can trigger undefined behavior via binding a reference to a null pointer or can access data outside the bounds of heap allocated arrays. The [implementation](https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/quantize_op.cc#L59) has some validation but does not check that `min_range` and `max_range` both have the same non-zero number of elements. If `axis` is provided (i.e., not `-1`), then validation should check that it is a value in range for the rank of `input` tensor and then the lengths of `min_range` and `max_range` inputs match the `axis` dimension of the `input` tensor. We have patched the issue in GitHub commit 6da6620efad397c85493b8f8667b821403516708. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, Te...</p> |
| Git | 2.45.2 | CVE-2021-37665 | ['HIGH', 'HIGH'] | [7.8, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions due to incomplete validation in MKL implementation of requantization, an attacker can trigger undefined behavior via binding a reference to a null pointer or can access data outside the bounds of heap allocated arrays. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/mkl/mkl_requantization_range_per_channel_op.cc) does not validate the dimensions of the `input` tensor. A similar issue occurs in `MklRequantizePerChannelOp`. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/mkl/mkl_requantize_per_channel_op.cc) does not perform full validation for all the input arguments. We have patched the issue in GitHub commit 9e62869465573cb2d9b5053f1fa02a81fce21d69 and in the Github commit 203214568f5bc237603dbab6e1fd389f1572f5c9. The fix will...</p>  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37668 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause denial of service in applications serving models using <code>`tf.raw_ops.UnravelIndex`</code> by triggering a division by 0. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/unravel_index_op.cc#L36) does not check that the tensor subsumed by <code>`dims`</code> is not empty. Hence, if one element of <code>`dims`</code> is 0, the implementation does a division by 0. We have patched the issue in GitHub commit a776040a5e7ebf76eeb7eb923bf1ae417dd4d233. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37669 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause denial of service in applications serving models using <code>`tf.raw_ops.NonMaxSuppressionV5`</code> by triggering a division by 0. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/image/non_max_suppression_op.cc#L170-L271) uses a user controlled argument to resize a <code>`std::vector`</code>. However, as <code>`std::vector::resize`</code> takes the size argument as a <code>`size_t`</code> and <code>`output_size`</code> is an <code>`int`</code>, there is an implicit conversion to unsigned. If the attacker supplies a negative value, this conversion results in a crash. A similar issue occurs in <code>`CombinedNonMaxSuppression`</code>. We have patched the issue in GitHub commit 3a7362750d5c372420aa8f0caf7bf5b5c3d0f52d and commit [b5cdbf12ffcaaffecf98f22a6be5a64bb96e4f58]. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorF...</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37670 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can read from outside of bounds of heap allocated data by sending specially crafted illegal arguments to `tf.raw_ops.UpperBound`. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/searchsorted_op.cc#L85-L104) does not validate the rank of `sorted_input` argument. A similar issue occurs in `tf.raw_ops.LowerBound`. We have patched the issue in GitHub commit 42459e4273c2e47a3232cc16c4f4ff3b3a35c38. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range. |
| Git | 2.45.2 | CVE-2021-37672 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can read from outside of bounds of heap allocated data by sending specially crafted illegal arguments to `tf.raw_ops.SdcaOptimizerV2`. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/sdca_internal.cc#L320-L353) does not check that the length of `example_labels` is the same as the number of examples. We have patched the issue in GitHub commit a4e138660270e7599793fa438cd7b2fc2ce215a6. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.            |
| Git | 2.45.2 | CVE-2021-37673 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.MapStage`. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/map_stage_op.cc#L513) does not check that the `key` input is a valid non-empty tensor. We have patched the issue in GitHub commit d7de67733925de196ec8863a33445b73f9562d1d. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37674 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a denial of service via a segmentation fault in `tf.raw_ops.MaxPoolGrad` caused by missing validation. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/maxpooling_op.cc) misses some validation for the `orig_input` and `orig_output` tensors. The fixes for CVE-2021-29579 were incomplete. We have patched the issue in GitHub commit 136b51f10903e044308cf77117c0ed9871350475. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37677 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the shape inference code for `tf.raw_ops.Dequantize` has a vulnerability that could trigger a denial of service via a segfault if an attacker provides invalid arguments. The shape inference [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/ops/array_ops.cc#L2999-L3014) uses `axis` to select between two different values for `minmax_rank` which is then used to retrieve tensor dimensions. However, code assumes that `axis` can be either `-1` or a value greater than `-1`, with no validation for the other values. We have patched the issue in GitHub commit da857cfa0fde8f79ad0afdbc94e88b5d4bbec764. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37678 | ['CRITICAL', 'HIGH'] | [9.3, 8.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions TensorFlow and Keras can be tricked to perform arbitrary code execution when deserializing a Keras model from YAML format. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/python/keras/saving/model_config.py#L66-L104) uses `yaml.unsafe_load` which can perform arbitrary code execution on the input. Given that YAML format support requires a significant amount of work, we have removed it for now. We have patched the issue in GitHub commit 23d6383eb6c14084a8fc3bdf164043b974818012. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37679 | ['HIGH', 'HIGH']     | [7.1, 7.8] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions it is possible to nest a `tf.map_fn` within another `tf.map_fn` call. However, if the input tensor is a `RaggedTensor` and there is no function signature provided, code assumes the output is a fully specified tensor and fills output buffer with uninitialized contents from the heap. The `t` and `z` outputs should be identical, however this is not the case. The last row of `t` contains data from the heap which can be used to leak other memory information. The bug lies in the conversion from a `Variant` tensor to a `RaggedTensor`. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/ragged_tensor_from_variant_op.cc#L177-L190) does not check that all inner shapes match and this results in the additional dimensions. The same implementation can result in data loss, if input tensor is tweaked. We have patched the issue in...</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-37682 | ['MEDIUM', 'HIGH']   | [4.4, 7.1] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions all TFLite operations that use quantization can be made to use uninitialized values. [For example](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/depthwise_conv.cc#L198-L200). The issue stems from the fact that `quantization.params` is only valid if `quantization.type` is different that `kTfLiteNoQuantization`. However, these checks are missing in large parts of the code. We have patched the issue in GitHub commits 537bc7c723439b9194a358f64d871dd326c18887, 4a91f2069f7145aab6ba2d8cfe41be8a110c18a5 and 8933b8a21280696ab119b63263babdb54c298538. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |
| Git | 2.45.2 | CVE-2021-37683 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of division in TFLite is [vulnerable to a division by 0 error](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/div.cc). There is no check that the divisor tensor does not contain zero elements. We have patched the issue in GitHub commit 1e206baedf8bef0334cca3eb92bab134ef525a28. The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37684 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementations of pooling in TFLite are vulnerable to division by 0 errors as there are no checks for divisors not being 0. We have patched the issue in GitHub commit [dfa22b348b70bb89d6d6ec0ff53973bacb4f4695](https://github.com/tensorflow/tensorflow/commit/dfa22b348b70bb89d6d6ec0ff53973bacb4f4695). The fix will be included in TensorFlow 2.6.0. We will also cherry-pick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37685 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions TFLite's <code>['expand_dims.cc']</code>(<a href="https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/expand_dims.cc#L36-L50">https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/expand_dims.cc#L36-L50</a>) contains a vulnerability which allows reading one element outside of bounds of heap allocated data. If <code>`axis`</code> is a large negative value (e.g., <code>`-100000`</code>), then after the first <code>`if`</code> it would still be negative. The check following the <code>`if`</code> statement will pass and the <code>`for`</code> loop would read one element before the start of <code>`input_dims.data`</code> (when <code>`i = 0`</code>). We have patched the issue in GitHub commit <code>d94ffe08a65400f898241c0374e9edc6fa8ed257</code>. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>  |
| Git | 2.45.2 | CVE-2021-37687 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions TFLite's <code>['GatherNd` implementation']</code>(<a href="https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/gather_nd.cc#L124">https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/gather_nd.cc#L124</a>) does not support negative indices but there are no checks for this situation. Hence, an attacker can read arbitrary data from the heap by carefully crafting a model with negative values in <code>`indices`</code>. Similar issue exists in <code>['Gather` implementation']</code>(<a href="https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/gather.cc">https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/gather.cc</a>). We have patched the issue in GitHub commits <code>bb6a0383ed553c286f87ca88c207f6774d5c4a8f</code> and <code>eb921122119a6b6e470ee98b89e65d721663179d</code>. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p> |
| Git | 2.45.2 | CVE-2021-37691 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | <p>TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can craft a TFLite model that would trigger a division by zero error in LSH <code>[implementation]</code>(<a href="https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/lsh_projection.cc#L118">https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/lsh_projection.cc#L118</a>). We have patched the issue in GitHub commit <code>0575b640091680cfb70f4dd93e70658de43b94f9</code>. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.</p>   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-37692 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions under certain conditions, Go code can trigger a segfault in string deallocation. For string tensors, `C.TF_TString_Dealloc` is called during garbage collection within a finalizer function. However, tensor structure isn't checked until encoding to avoid a performance penalty. The current method for dealloc assumes that encoding succeeded, but segfaults when a string tensor is garbage collected whose encoding failed (e.g., due to mismatched dimensions). To fix this, the call to set the finalizer function is deferred until `NewTensor` returns and, if encoding failed for a string tensor, deallocs are determined based on bytes written. We have patched the issue in GitHub commit 8721ba96e5760c229217b594f6d2ba332beedf22. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, which is the other affected version.  |
| Git | 2.45.2 | CVE-2021-37690 | ['MEDIUM', 'MEDIUM'] | [6.6, 6.6] | TensorFlow is an end-to-end open source platform for machine learning. In affected versions when running shape functions, some functions (such as `MutableHashTableShape`) produce extra output information in the form of a `ShapeAndType` struct. The shapes embedded in this struct are owned by an inference context that is cleaned up almost immediately; if the upstream code attempts to access this shape information, it can trigger a segfault. `ShapeRefiner` is mitigating this for normal output shapes by cloning them (and thus putting the newly created shape under ownership of an inference context that will not die), but we were not doing the same for shapes and types. This commit fixes that by doing similar logic on output shapes and types. We have patched the issue in GitHub commit ee119d4a498979525046fba1c3dd3f13a039fbb1. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected. |
| Git | 2.45.2 | CVE-2021-38711 | HIGH                 | 7.5        | In gitit before 0.15.0.0, the Export feature can be exploited to leak information from files.  |
| Git | 2.45.2 | CVE-2020-18900 | ['LOW', 'LOW']       | [3.3, 3.3] | A heap-based buffer overflow in the libexe_io_handle_read_coff_optional_header function of libyal libexe before 20181128. NOTE: the vendor has disputed this as described in libyal/libexe issue 1 on GitHub   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-22238 | ['MEDIUM', 'MEDIUM'] | [6.8, 5.4] | An issue has been discovered in GitLab affecting all versions starting with 13.3. GitLab was vulnerable to a stored XSS by using the design feature in issues.  |
| Git | 2.45.2 | CVE-2021-22246 | ['HIGH', 'MEDIUM']   | [7.7, 6.5] | A vulnerability was discovered in GitLab versions before 14.0.2, 13.12.6, 13.11.6. GitLab Webhook feature could be abused to perform denial of service attacks.   |
| Git | 2.45.2 | CVE-2021-22254 | ['LOW', 'MEDIUM']    | [3.1, 4.3] | Under very specific conditions a user could be impersonated using Gitlab shell. This vulnerability affects GitLab CE/EE 13.1 and later through 14.1.2, 14.0.7 and 13.12.9.  |
| Git | 2.45.2 | CVE-2021-22248 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Improper authorization on the pipelines page in GitLab CE/EE affecting all versions since 13.12 allowed unauthorized users to view some pipeline information for public projects that have access to pipelines restricted to members only   |
| Git | 2.45.2 | CVE-2021-22249 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | A verbose error message in GitLab EE affecting all versions since 12.2 could disclose the private email address of a user invited to a group  |
| Git | 2.45.2 | CVE-2021-22251 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper validation of invited users' email address in GitLab EE affecting all versions since 12.2 allowed projects to add members with email address domain that should be blocked by group settings   |
| Git | 2.45.2 | CVE-2021-22252 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | A confusion between tag and branch names in GitLab CE/EE affecting all versions since 13.7 allowed a Developer to access protected CI variables which should only be accessible to Maintainers  |
| Git | 2.45.2 | CVE-2021-22253 | ['MEDIUM', 'MEDIUM'] | [4.9, 5.4] | Improper authorization in GitLab EE affecting all versions since 13.4 allowed a user who previously had the necessary access to trigger deployments to protected environments under specific conditions after the access has been removed   |
| Git | 2.45.2 | CVE-2021-39160 | ['CRITICAL', 'HIGH'] | [9.6, 8.8] | nbgitpuller is a Jupyter server extension to sync a git repository one-way to a local path. Due to unsanitized input, visiting maliciously crafted links could result in arbitrary code execution in the user environment. This has been resolved in version 0.10.2 and all users are advised to upgrade. No work around exist for users who can not upgrade. |
| Git | 2.45.2 | CVE-2021-22236 | ['MEDIUM', 'HIGH']   | [5.5, 8.8] | Due to improper handling of OAuth client IDs, new subscriptions generated OAuth tokens on an incorrect OAuth client application. This vulnerability is present in GitLab CE/EE since version 14.1.  |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22237 | ['MEDIUM', 'MEDIUM']     | [6.6, 4.9] | Under specialized conditions, GitLab may allow a user with an impersonation token to perform Git actions even if impersonation is disabled. This vulnerability is present in GitLab CE/EE versions before 13.12.9, 14.0.7, 14.1.2  |
| Git | 2.45.2 | CVE-2021-22242 | ['HIGH', 'MEDIUM']       | [8.7, 5.4] | Insufficient input sanitization in Mermaid markdown in GitLab CE/EE version 11.4 and up allows an attacker to exploit a stored cross-site scripting vulnerability via a specially-crafted markdown   |
| Git | 2.45.2 | CVE-2021-22243 | ['MEDIUM', 'MEDIUM']     | [5.0, 4.3] | Under specialized conditions, GitLab CE/EE versions starting 7.10 may allow existing GitLab users to use an invite URL meant for another email address to gain access into a group.  |
| Git | 2.45.2 | CVE-2021-22244 | ['LOW', 'MEDIUM']        | [3.1, 6.5] | Improper authorization in the vulnerability report feature in GitLab EE affecting all versions since 13.1 allowed a reporter to access vulnerability data  |
| Git | 2.45.2 | CVE-2021-22245 | ['LOW', 'LOW']           | [2.7, 2.7] | Improper validation of commit author in GitLab CE/EE affecting all versions allowed an attacker to make several pages in a project impossible to view  |
| Git | 2.45.2 | CVE-2021-22247 | ['MEDIUM', 'MEDIUM']     | [4.3, 4.3] | Improper authorization in GitLab CE/EE affecting all versions since 13.0 allows guests in private projects to view CI/CD analytics   |
| Git | 2.45.2 | CVE-2021-22250 | ['MEDIUM', 'MEDIUM']     | [5.4, 5.4] | Improper authorization in GitLab CE/EE affecting all versions since 13.3 allowed users to view and delete impersonation tokens that administrators created for their account   |
| Git | 2.45.2 | CVE-2021-22256 | ['MEDIUM', 'MEDIUM']     | [5.4, 5.4] | Improper authorization in GitLab CE/EE affecting all versions since 12.6 allowed guest users to create issues for Sentry errors and track their status   |
| Git | 2.45.2 | CVE-2021-39159 | ['CRITICAL', 'CRITICAL'] | [9.6, 9.8] | BinderHub is a kubernetes-based cloud service that allows users to share reproducible interactive computing environments from code repositories. In affected versions a remote code execution vulnerability has been identified in BinderHub, where providing BinderHub with maliciously crafted input could execute code in the BinderHub context, with the potential to egress credentials of the BinderHub deployment, including JupyterHub API tokens, kubernetes service accounts, and docker registry credentials. This may provide the ability to manipulate images and other user created pods in the deployment, with the potential to escalate to the host depending on the underlying kubernetes configuration. Users are advised to update to version 0.2.0-n653. If users are unable to update they may disable the git repo provider by specifying the `BinderHub.repo_providers` as a workaround. |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-40330 | HIGH                 | 7.5        | git_connect_git in connect.c in Git before 2.30.1 allows a repository path to contain a newline character, which may result in unexpected cross-protocol requests, as demonstrated by the git://localhost:1234/%0d%0a%0d%0aGET%20/%20 HTTP/1.1 substring.  |
| Git | 2.45.2 | CVE-2021-39135 | ['HIGH', 'HIGH']     | [8.2, 7.8] | `@npmcli/arborist`, the library that calculates dependency trees and manages the node_modules folder hierarchy for the npm command line interface, aims to guarantee that package dependency contracts will be met, and the extraction of package contents will always be performed into the expected folder. This is accomplished by extracting package contents into a project's `node_modules` folder. If the `node_modules` folder of the root project or any of its dependencies is somehow replaced with a symbolic link, it could allow Arborist to write package dependencies to any arbitrary location on the file system. Note that symbolic links contained within package artifact contents are filtered out, so another means of creating a `node_modules` symbolic link would have to be employed. 1. A `preinstall` script could replace `node_modules` with a symlink. (This is prevented by using `--ignore-scripts`.) 2. An attacker could supply the target with a git repository, instructing them to run `npm in... |
| Git | 2.45.2 | CVE-2021-39185 | CRITICAL             | 9.1        | Http4s is a minimal, idiomatic Scala interface for HTTP services. In http4s versions 0.21.26 and prior, 0.22.0 through 0.22.2, 0.23.0, 0.23.1, and 1.0.0-M1 through 1.0.0-M24, the default CORS configuration is vulnerable to an origin reflection attack. The middleware is also susceptible to a Null Origin Attack. The problem is fixed in 0.21.27, 0.22.3, 0.23.2, and 1.0.0-M25. The original `CORS` implementation and `CORSConfig` are deprecated. See the GitHub GHSA for more information, including code examples and workarounds.   |
| Git | 2.45.2 | CVE-2021-22239 | ['MEDIUM', 'MEDIUM'] | [5.0, 4.3] | An unauthorized user was able to insert metadata when creating new issue on GitLab CE/EE 14.0 and later.   |

|     |        |                |                        |            |   |
|-----|--------|----------------|------------------------|------------|---|
| Git | 2.45.2 | CVE-2021-32724 | CRITICAL               | 9.9        | <p>check-spelling is a github action which provides CI spell checking. In affected versions and for a repository with the [check-spelling action](https://github.com/marketplace/actions/check-spelling) enabled that triggers on `pull_request_target` (or `schedule`), an attacker can send a crafted Pull Request that causes a `GITHUB_TOKEN` to be exposed. With the `GITHUB_TOKEN`, it's possible to push commits to the repository bypassing standard approval processes. Commits to the repository could then steal any/all secrets available to the repository. As a workaround users may can either: [Disable the workflow](https://docs.github.com/en/actions/managing-workflow-runs/disabling-and-enabling-a-workflow) until you've fixed all branches or Set repository to [Allow specific actions](https://docs.github.com/en/github/administering-a-repository/managing-repository-settings/disabling-or-limiting-github-actions-for-a-repository#allowing-specific-actions-to-run). check-spelling isn't a verified crea...</p> |
| Git | 2.45.2 | CVE-2021-41077 | HIGH                   | 7.5        | <p>The activation process in Travis CI, for certain 2021-09-03 through 2021-09-10 builds, causes secret data to have unexpected sharing that is not specified by the customer-controlled .travis.yml file. In particular, the desired behavior (if .travis.yml has been created locally by a customer, and added to git) is for a Travis service to perform builds in a way that prevents public access to customer-specific secret environment data such as signing keys, access credentials, and API tokens. However, during the stated 8-day interval, secret data could be revealed to an unauthorized actor who forked a public repository and printed files during a build process.</p>   |
| Git | 2.45.2 | CVE-2021-39227 | ['MEDIUM', 'CRITICAL'] | [6.2, 9.8] | <p>ZRender is a lightweight graphic library providing 2d draw for Apache ECharts. In versions prior to 5.2.1, using `merge` and `clone` helper methods in the `src/core/util.ts` module results in prototype pollution. It affects the popular data visualization library Apache ECharts, which uses and exports these two methods directly. The GitHub Security Advisory page for this vulnerability contains a proof of concept. This issue is patched in ZRender version 5.2.1. One workaround is available: Check if there is `__proto__` in the object keys. Omit it before using it as an parameter in these affected methods. Or in `echarts.util.merge` and `setOption` if project is using ECharts.</p>  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22868 | MEDIUM               | 4.3        | A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This vulnerability was reported via the GitHub Bug Bounty program. This is the result of an incomplete fix for CVE-2021-22867. |
| Git | 2.45.2 | CVE-2021-22869 | CRITICAL             | 9.8        | An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in 3.0.16 and 3.1.8 releases.  |
| Git | 2.45.2 | CVE-2021-22259 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | A potential DOS vulnerability was discovered in GitLab EE starting with version 12.6 due to lack of pagination in dependencies API.  |
| Git | 2.45.2 | CVE-2021-39868 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE since version 8.12, an authenticated low-privileged malicious user may create a project with unlimited repository size by modifying values in a project export.  |
| Git | 2.45.2 | CVE-2021-39871 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE since version 13.0, an instance that has the setting to disable Bitbucket Server import enabled is bypassed by an attacker making a crafted API call.  |
| Git | 2.45.2 | CVE-2021-39873 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE, there exists a content spoofing vulnerability which may be leveraged by attackers to trick users into visiting a malicious website by spoofing the content in an error response.  |
| Git | 2.45.2 | CVE-2021-39874 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE since version 11.0, the requirement to enforce 2FA is not honored when using git commands.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-39877 | ['HIGH', 'MEDIUM']   | [7.7, 5.5] | A vulnerability was discovered in GitLab starting with version 12.2 that allows an attacker to cause uncontrolled resource consumption with a specially crafted file.  |
| Git | 2.45.2 | CVE-2021-39879 | ['LOW', 'LOW']       | [2.2, 3.5] | Missing authentication in all versions of GitLab CE/EE since version 7.11.0 allows an attacker with access to a victim's session to disable two-factor authentication  |
| Git | 2.45.2 | CVE-2021-39883 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper authorization checks in all versions of GitLab EE starting from 13.11 before 14.1.7, all versions starting from 14.2 before 14.2.5, and all versions starting from 14.3 before 14.3.1 allows subgroup members to see epics from all parent subgroups.   |
| Git | 2.45.2 | CVE-2021-39885 | ['HIGH', 'MEDIUM']   | [8.7, 5.4] | A Stored XSS in merge request creation page in all versions of Gitlab EE starting from 13.7 before 14.1.7, all versions starting from 14.2 before 14.2.5, and all versions starting from 14.3 before 14.3.1 allows an attacker to execute arbitrary JavaScript code on the victim's behalf via malicious approval rule names   |
| Git | 2.45.2 | CVE-2021-39896 | ['LOW', 'LOW']       | [3.8, 3.8] | In all versions of GitLab CE/EE since version 8.0, when an admin uses the impersonate feature twice and stops impersonating, the admin may be logged in as the second user they impersonated, which may lead to repudiation issues.  |
| Git | 2.45.2 | CVE-2021-39899 | ['LOW', 'MEDIUM']    | [2.9, 4.2] | In all versions of GitLab CE/EE, an attacker with physical access to a user's machine may brute force the user's password via the change password function. There is a rate limit in place, but the attack may still be conducted by stealing the session id from the physical compromise of the account and splitting the attack over several IP addresses and passing in the compromised session value from these various locations. |
| Git | 2.45.2 | CVE-2021-39900 | ['LOW', 'LOW']       | [2.0, 2.7] | Information disclosure from SendEntry in GitLab starting with 10.8 allowed exposure of full URL of artifacts stored in object-storage with a temporary availability via Rails logs.  |
| Git | 2.45.2 | CVE-2021-39887 | ['HIGH', 'MEDIUM']   | [7.3, 5.4] | A stored Cross-Site Scripting vulnerability in the GitLab Flavored Markdown in GitLab CE/EE version 8.4 and above allowed an attacker to execute arbitrary JavaScript code on the victim's behalf.   |
| Git | 2.45.2 | CVE-2021-39866 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | A business logic error in the project deletion process in GitLab 13.6 and later allows persistent access via project access tokens.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-39867 | ['MEDIUM', 'HIGH']   | [6.5, 8.1] | In all versions of GitLab CE/EE since version 8.15, a DNS rebinding vulnerability in Gitea Importer may be exploited by an attacker to trigger Server Side Request Forgery (SSRF) attacks.   |
| Git | 2.45.2 | CVE-2021-39869 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | In all versions of GitLab CE/EE since version 8.9, project exports may expose trigger tokens configured on that project.   |
| Git | 2.45.2 | CVE-2021-39872 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | In all versions of GitLab CE/EE since version 14.1, an improper access control vulnerability allows users with expired password to still access GitLab through git and API through access tokens acquired before password expiration.  |
| Git | 2.45.2 | CVE-2021-39875 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | In all versions of GitLab CE/EE since version 13.6, it is possible to see pending invitations of any public group or public project by visiting an API endpoint.   |
| Git | 2.45.2 | CVE-2021-39878 | ['MEDIUM', 'MEDIUM'] | [5.8, 5.4] | A stored Reflected Cross-Site Scripting vulnerability in the Jira integration in GitLab version 13.0 up to 14.3.1 allowed an attacker to execute arbitrary javascript code.  |
| Git | 2.45.2 | CVE-2021-39882 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | In all versions of GitLab CE/EE, provided a user ID, anonymous users can use a few endpoints to retrieve information about any GitLab user.  |
| Git | 2.45.2 | CVE-2021-39884 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab EE since version 8.13, an endpoint discloses names of private groups that have access to a project to low privileged users that are part of that project.  |
| Git | 2.45.2 | CVE-2021-39888 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab EE starting from 13.10 before 14.1.7, all versions starting from 14.2 before 14.2.5, and all versions starting from 14.3 before 14.3.1 a specific API endpoint may reveal details about a private group and other sensitive info inside issue and merge request templates.                                   |
| Git | 2.45.2 | CVE-2021-39893 | ['MEDIUM', 'HIGH']   | [5.3, 7.5] | A potential DOS vulnerability was discovered in GitLab starting with version 9.1 that allowed parsing files without authorisation.   |
| Git | 2.45.2 | CVE-2021-39894 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | In all versions of GitLab CE/EE since version 8.0, a DNS rebinding vulnerability exists in Fogbugz importer which may be used by attackers to exploit Server Side Request Forgery attacks.   |
| Git | 2.45.2 | CVE-2021-22257 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. The route for /user.keys is not restricted on instances with public visibility disabled. This allows user enumeration on such instances. |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-22258 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | The project import/export feature in GitLab 8.9 and greater could be used to obtain otherwise private email addresses  |
| Git | 2.45.2 | CVE-2021-22261 | ['HIGH', 'MEDIUM']   | [7.3, 4.8] | A stored Cross-Site Scripting vulnerability in the Jira integration in all GitLab versions starting from 13.9 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 allows an attacker to execute arbitrary JavaScript code on the victim's behalf via malicious Jira API responses  |
| Git | 2.45.2 | CVE-2021-22262 | ['MEDIUM', 'MEDIUM'] | [5.4, 4.3] | Missing access control in all GitLab versions starting from 13.12 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 with Jira Cloud integration enabled allows Jira users without administrative privileges to add and remove Jira Connect Namespaces via the GitLab.com for Jira Cloud application configuration page |
| Git | 2.45.2 | CVE-2021-22264 | ['MEDIUM', 'MEDIUM'] | [6.8, 6.5] | An issue has been discovered in GitLab affecting all versions starting from 13.8 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. Under specialized conditions, an invited group member may continue to have access to a project even after the invited group, which the member was part of, is deleted.                 |
| Git | 2.45.2 | CVE-2021-39870 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE since version 11.11, an instance that has the setting to disable Repo by URL import enabled is bypassed by an attacker making a crafted API call.  |
| Git | 2.45.2 | CVE-2021-39881 | ['LOW', 'LOW']       | [3.5, 3.5] | In all versions of GitLab CE/EE since version 7.7, the application may let a malicious user create an OAuth client application with arbitrary scope names which may allow the malicious user to trick unsuspecting users to authorize the malicious client application using the spoofed scope name and description.   |
| Git | 2.45.2 | CVE-2021-39886 | ['LOW', 'MEDIUM']    | [2.6, 4.3] | Permissions rules were not applied while issues were moved between projects of the same group in GitLab versions starting with 10.6 and up to 14.1.7 allowing users to read confidential Epic references.  |
| Git | 2.45.2 | CVE-2021-39889 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab EE since version 14.1, due to an insecure direct object reference vulnerability, an endpoint may reveal the protected branch name to a malicious user who makes a crafted API call with the ID of the protected branch.  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-39891 | ['MEDIUM', 'MEDIUM'] | [5.9, 4.9] | In all versions of GitLab CE/EE since version 8.0, access tokens created as part of admin's impersonation of a user are not cleared at the end of impersonation which may lead to unnecessary sensitive info disclosure.  |
| Git | 2.45.2 | CVE-2021-39880 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | A Denial Of Service vulnerability in the apollo_upload_server Ruby gem in GitLab CE/EE all versions starting from 11.9 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 allows an attacker to deny access to all users via specially crafted requests to the apollo_upload_server middleware.  |
| Git | 2.45.2 | CVE-2021-21684 | MEDIUM               | 6.1        | Jenkins Git Plugin 4.8.2 and earlier does not escape the Git SHA-1 checksum parameters provided to commit notifications when displaying them in a build cause, resulting in a stored cross-site scripting (XSS) vulnerability.  |
| Git | 2.45.2 | CVE-2021-42091 | CRITICAL             | 9.1        | An issue was discovered in Zammad before 4.1.1. SSRF can occur via GitHub or GitLab integration.  |
| Git | 2.45.2 | CVE-2021-22263 | ['MEDIUM', 'MEDIUM'] | [5.5, 6.5] | An issue has been discovered in GitLab affecting all versions starting from 13.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. A user account with 'external' status which is granted 'Maintainer' role on any project on the GitLab instance where 'project tokens' are allowed may elevate its privilege to 'Internal' and access Internal projects. |
| Git | 2.45.2 | CVE-2021-42341 | HIGH                 | 7.5        | checkpath in OpenRC before 0.44.7 uses the direct output of strlen() to allocate strings, which does not account for the '\0' byte at the end of the string. This results in memory corruption. CVE-2021-42341 was introduced in git commit 63db2d99e730547339d1bd d28e8437999c380cae, which was introduced as part of OpenRC 0.44.0 development.   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-41168 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | <p>Snudown is a reddit-specific fork of the Sundown Markdown parser used by GitHub, with Python integration added. In affected versions snudown was found to be vulnerable to denial of service attacks to its reference table implementation. References written in markdown `[reference_name]: https://www.example.com` are inserted into a hash table which was found to have a weak hash function, meaning that an attacker can reliably generate a large number of collisions for it. This makes the hash table vulnerable to a hash-collision DoS attack, a type of algorithmic complexity attack. Further the hash table allowed for duplicate entries resulting in long retrieval times. Proofs of concept and further discussion of the hash collision issue are discussed on the snudown GHSA(<a href="https://github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6">https://github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6</a>). Users are advised to update to version 1.7.0.</p>                   |
| Git | 2.45.2 | CVE-2021-41188 | ['MEDIUM', 'MEDIUM'] | [5.7, 5.4] | <p>Shopware is open source e-commerce software. Versions prior to 5.7.6 contain a cross-site scripting vulnerability. This issue is patched in version 5.7.6. Two workarounds are available. Using the security plugin or adding a particular following config to the `.htaccess` file will protect against cross-site scripting in this case. There is also a config for those using nginx as a server. The plugin and the configs can be found on the GitHub Security Advisory page for this vulnerability.</p>   |
| Git | 2.45.2 | CVE-2021-41238 | ['HIGH', 'HIGH']     | [8.6, 7.5] | <p>Hangfire is an open source system to perform background job processing in a .NET or .NET Core applications. No Windows Service or separate process required. Dashboard UI in Hangfire.Core uses authorization filters to protect it from showing sensitive data to unauthorized users. By default when no custom authorization filters specified, `LocalRequestsOnlyAuthorizationFilter` filter is being used to allow only local requests and prohibit all the remote requests to provide sensible, protected by default settings. However due to the recent changes, in version 1.7.25 no authorization filters are used by default, allowing remote requests to succeed. If you are using `UseHangfireDashboard` method with default `DashboardOptions.Authorization` property value, then your installation is impacted. If any other authorization filter is specified in the `DashboardOptions.Authorization` property, the you are not impacted. Patched versions (1.7.26) are available both on Nuget.org and as a tagged rel...</p> |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-39902 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Incorrect Authorization in GitLab CE/EE 13.4 or above allows a user with guest membership in a project to modify the severity of an incident.  |
| Git | 2.45.2 | CVE-2021-39903 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | In all versions of GitLab CE/EE since version 13.0, a privileged user, through an API call, can change the visibility level of a group or a project to a restricted option even after the instance administrator sets that visibility option as restricted in settings.  |
| Git | 2.45.2 | CVE-2021-39914 | ['LOW', 'MEDIUM']    | [3.1, 4.3] | A regular expression denial of service issue in GitLab versions 8.13 to 14.2.5, 14.3.0 to 14.3.3 and 14.4.0 could cause excessive usage of resources when a specially crafted username was used when provisioning a new user   |
| Git | 2.45.2 | CVE-2021-22260 | ['HIGH', 'MEDIUM']   | [7.7, 5.4] | A stored Cross-Site Scripting vulnerability in the DataDog integration in all versions of GitLab CE/EE starting from 13.7 before 14.0.9, all versions starting from 14.1 before 14.1.4, and all versions starting from 14.2 before 14.2.2 allows an attacker to execute arbitrary JavaScript code on the victim's behalf                                       |
| Git | 2.45.2 | CVE-2021-39895 | ['MEDIUM', 'MEDIUM'] | [6.0, 4.5] | In all versions of GitLab CE/EE since version 8.0, an attacker can set the pipeline schedules to be active in a project export so when an unsuspecting owner imports that project, pipelines are active by default on that project. Under specialized conditions, this may lead to information disclosure if the project is imported from an untrusted source. |
| Git | 2.45.2 | CVE-2021-39897 | ['LOW', 'MEDIUM']    | [2.6, 5.3] | Improper access control in GitLab CE/EE version 10.5 and above allowed subgroup members with inherited access to a project from a parent group to still have access even after the subgroup is transferred   |
| Git | 2.45.2 | CVE-2021-39898 | ['LOW', 'MEDIUM']    | [3.7, 5.3] | In all versions of GitLab CE/EE since version 10.6, a project export leaks the external webhook token value which may allow access to the project which it was exported from.  |
| Git | 2.45.2 | CVE-2021-39901 | ['LOW', 'LOW']       | [2.7, 2.7] | In all versions of GitLab CE/EE since version 11.10, an admin of a group can see the SCIM token of that group by visiting a specific endpoint.   |
| Git | 2.45.2 | CVE-2021-39904 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An Improper Access Control vulnerability in the GraphQL API in all versions of GitLab CE/EE starting from 13.1 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows a Merge Request creator to resolve discussions and apply suggestions after a project owner has locked the Merge Request  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-39905 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An information disclosure vulnerability in the GitLab CE/EE API since version 8.9.6 allows a user to see basic information on private groups that a public project has been shared with  |
| Git | 2.45.2 | CVE-2021-39906 | ['HIGH', 'MEDIUM']   | [8.7, 6.1] | Improper validation of ipynb files in GitLab CE/EE version 13.5 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf.  |
| Git | 2.45.2 | CVE-2021-39907 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | A potential DOS vulnerability was discovered in GitLab CE/EE starting with version 13.7. The stripping of EXIF data from certain images resulted in high CPU usage.  |
| Git | 2.45.2 | CVE-2021-39909 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab EE starting from 11.3 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows an attacker to bypass CODEOWNERS Merge Request approval requirement under rare circumstances   |
| Git | 2.45.2 | CVE-2021-39911 | ['LOW', 'MEDIUM']    | [1.7, 4.3] | An improper access control flaw in all versions of GitLab CE/EE starting from 13.9 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 exposes private email address of Issue and Merge Requests assignee to Webhook data consumers  |
| Git | 2.45.2 | CVE-2021-39912 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | A potential DoS vulnerability was discovered in GitLab CE/EE starting with version 13.7. Using a malformed TIFF images was possible to trigger memory exhaustion.  |
| Git | 2.45.2 | CVE-2021-39913 | ['MEDIUM', 'MEDIUM'] | [4.4, 6.7] | Accidental logging of system root password in the migration log in all versions of GitLab CE/EE before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows an attacker with local file system access to obtain system root-level privileges  |
| Git | 2.45.2 | CVE-2021-22870 | MEDIUM               | 6.5        | A path traversal vulnerability was identified in GitHub Pages builds on GitHub Enterprise Server that could allow an attacker to read system files. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.0.19, 3.1.11, and 3.2.3. This vulnerability was reported via the GitHub Bug Bounty program. |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2021-3572  | MEDIUM             | 5.7        | A flaw was found in python-pip in the way it handled Unicode separators in git references. A remote attacker could possibly use this issue to install a different revision on a repository. The highest threat from this vulnerability is to data integrity. This is fixed in python-pip version 21.1.   |
| Git | 2.45.2 | CVE-2021-41192 | ['HIGH', 'MEDIUM'] | [8.1, 6.5] | Redash is a package for data visualization and sharing. If an admin sets up Redash versions 10.0.0 and prior without explicitly specifying the `REDASH_COOKIE_SECRET` or `REDASH_SECRET_KEY` environment variables, a default value is used for both that is the same across all installations. In such cases, the instance is vulnerable to attackers being able to forge sessions using the known default value. This issue only affects installations where the `REDASH_COOKIE_SECRET` or `REDASH_SECRET_KEY` environment variables have not been explicitly set. This issue does not affect users of the official Redash cloud images, Redash's Digital Ocean marketplace droplets, or the scripts in the `getredash/setup` repository. These instances automatically generate unique secret keys during installation. One can verify whether one's instance is affected by checking the value of the `REDASH_COOKIE_SECRET` environment variable. If it is `c292a0a3aa32397cdb050e233733900f`, should follow the steps to secure t... |
| Git | 2.45.2 | CVE-2021-43780 | ['MEDIUM', 'HIGH'] | [6.8, 8.8] | Redash is a package for data visualization and sharing. In versions 10.0 and prior the implementation of URL-loading data sources like JSON, CSV, or Excel is vulnerable to advanced methods of Server Side Request Forgery (SSRF). These vulnerabilities are only exploitable on installations where a URL-loading data source is enabled. As of time of publication, the `master` and `release/10.x.x` branches address this by applying the Advocate library for making http requests instead of the requests library directly. Users should upgrade to version 10.0.1 to receive this patch. There are a few workarounds for mitigating the vulnerability without upgrading. One can disable the vulnerable data sources entirely, by adding the following env variable to one's configuration, making them unavailable inside the webapp. One can switch any data source of certain types (viewable in the GitHub Security Advisory) to be `View Only` for all groups on the Settings > Groups > Data Sources screen. For users...    |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-3769  | ['HIGH', 'CRITICAL'] | [7.5, 9.8] | # Vulnerability in `pygmalion`, `pygmalion-virtualenv` and `refined` themes<br>**Description**: these themes use `print -P` on user-supplied strings to print them to the terminal. All of them do that on git information, particularly the branch name, so if the branch has a specially-crafted name the vulnerability can be exploited. **Fixed in**: [b3ba9978](https://github.com/ohmyzsh/ohmyzsh/commit/b3ba9978). **Impacted areas**: - `pygmalion` theme. - `pygmalion-virtualenv` theme. - `refined` theme.   |
| Git | 2.45.2 | CVE-2021-34599 | ['HIGH', 'HIGH']     | [7.4, 7.4] | Affected versions of CODESYS Git in Versions prior to V1.1.0.0 lack certificate validation in HTTPS handshakes. CODESYS Git does not implement certificate validation by default, so it does not verify that the server provides a valid and trusted HTTPS certificate. Since the certificate of the server to which the connection is made is not properly verified, the server connection is vulnerable to a man-in-the-middle attack.  |
| Git | 2.45.2 | CVE-2021-22170 | ['MEDIUM', 'HIGH']   | [6.2, 7.5] | Assuming a database breach, nonce reuse issues in GitLab 11.6+ allows an attacker to decrypt some of the database's encrypted content   |
| Git | 2.45.2 | CVE-2021-39890 | ['LOW', 'CRITICAL']  | [3.1, 9.8] | It was possible to bypass 2FA for LDAP users and access some specific pages with Basic Authentication in GitLab 14.1.1 and above.   |
| Git | 2.45.2 | CVE-2021-43800 | ['HIGH', 'HIGH']     | [7.5, 7.5] | Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git). |
| Git | 2.45.2 | CVE-2021-44684 | CRITICAL             | 9.8        | naholyr github-todos 3.1.0 is vulnerable to command injection. The range argument for the _hook subcommand is concatenated without any validation, and is directly used by the exec function.   |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2021-44685 | CRITICAL | 9.8 | Git-it through 4.4.0 allows OS command injection at the Branches Aren't Just For Birds challenge step. During the verification process, it attempts to run the reflog command followed by the current branch name (which is not sanitized for execution).   |
| Git | 2.45.2 | CVE-2021-43805 | HIGH     | 7.5 | Solidus is a free, open-source ecommerce platform built on Rails. Versions of Solidus prior to 3.1.4, 3.0.4, and 2.11.13 have a denial of service vulnerability that could be exploited during a guest checkout. The regular expression used to validate a guest order's email was subject to exponential backtracking through a fragment like `a.a.` Versions 3.1.4, 3.0.4, and 2.11.13 have been patched to use a different regular expression. The maintainers added a check for email addresses that are no longer valid that will print information about any affected orders that exist. If a prompt upgrade is not an option, a workaround is available. It is possible to edit the file `config/application.rb` manually (with code provided by the maintainers in the GitHub Security Advisory) to check email validity. |
| Git | 2.45.2 | CVE-2021-37940 | MEDIUM   | 6.8 | An information disclosure via GET request server-side request forgery vulnerability was discovered with the Workplace Search Github Enterprise Server integration. Using this vulnerability, a malicious Workplace Search admin could use the GHES integration to view hosts that might not be publicly accessible.   |
| Git | 2.45.2 | CVE-2021-43798 | HIGH     | 7.5 | Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0.0-beta1 through 8.3.0 (except for patched versions) is vulnerable to directory traversal, allowing access to local files. The vulnerable URL path is: ` <grafana_host_url>/public/plugins//`, where is the plugin ID for any installed plugin. At no time has Grafana Cloud been vulnerable. Users are advised to upgrade to patched versions 8.0.7, 8.1.8, 8.2.7, or 8.3.1. The GitHub Security Advisory contains more information about vulnerable URL paths, mitigation, and the disclosure timeline.</grafana_host_url>   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-43809 | ['MEDIUM', 'HIGH']   | [6.7, 7.3] | <p>`Bundler` is a package for managing application dependencies in Ruby. In `bundler` versions before 2.2.33, when working with untrusted and apparently harmless `Gemfile`'s, it is not expected that they lead to execution of external code, unless that's explicit in the ruby code inside the `Gemfile` itself. However, if the `Gemfile` includes `gem` entries that use the `git` option with invalid, but seemingly harmless, values with a leading dash, this can be false. To handle dependencies that come from a Git repository instead of a registry, Bundler uses various commands, such as `git clone`. These commands are being constructed using user input (e.g. the repository URL). When building the commands, Bundler versions before 2.2.33 correctly avoid Command Injection vulnerabilities by passing an array of arguments instead of a command string. However, there is the possibility that a user input starts with a dash (`-`) and is therefore treated as an optional argument instead of a positional...</p> |
| Git | 2.45.2 | CVE-2021-43802 | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | <p>Etherpad is a real-time collaborative editor. In versions prior to 1.8.16, an attacker can craft an `*.etherpad` file that, when imported, might allow the attacker to gain admin privileges for the Etherpad instance. This, in turn, can be used to install a malicious Etherpad plugin that can execute arbitrary code (including system commands). To gain privileges, the attacker must be able to trigger deletion of `express-session` state or wait for old `express-session` state to be cleaned up. Core Etherpad does not delete any `express-session` state, so the only known attacks require either a plugin that can delete session state or a custom cleanup process (such as a cron job that deletes old `sessionstorage:*` records). The problem has been fixed in version 1.8.16. If users cannot upgrade to 1.8.16 or install patches manually, several workarounds are available. Users may configure their reverse proxies to reject requests to `/p/*import`, which will block all imports, not just `*.ether...</p>  |
| Git | 2.45.2 | CVE-2021-39910 | ['LOW', 'MEDIUM']    | [2.6, 4.3] | <p>An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. GitLab was vulnerable to HTML Injection through the Swagger UI feature.</p>  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-39915 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Improper access control in the GraphQL API in GitLab CE/EE affecting all versions starting from 13.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker to see the names of project access tokens on arbitrary projects                                   |
| Git | 2.45.2 | CVE-2021-39916 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Lack of an access control check in the External Status Check feature allowed any authenticated user to retrieve the configuration of any External Status Check in GitLab EE starting from 14.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2.                            |
| Git | 2.45.2 | CVE-2021-39917 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.9 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. A regular expression related to quick actions features was susceptible to catastrophic backtracking that could cause a DOS attack. |
| Git | 2.45.2 | CVE-2021-39918 | ['LOW', 'MEDIUM']    | [3.1, 4.3] | Incorrect Authorization in GitLab EE affecting all versions starting from 11.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows a user to add comments to a vulnerability which cannot be accessed.   |
| Git | 2.45.2 | CVE-2021-39919 | ['MEDIUM', 'MEDIUM'] | [4.4, 4.4] | In all versions of GitLab CE/EE starting version 14.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, the reset password token and new user email token are accidentally logged which may lead to information disclosure.   |
| Git | 2.45.2 | CVE-2021-39930 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Missing authorization in GitLab EE versions between 12.4 and 14.3.6, between 14.4.0 and 14.4.4, and between 14.5.0 and 14.5.2 allowed an attacker to access a user's custom project and group templates  |
| Git | 2.45.2 | CVE-2021-39931 | ['LOW', 'MEDIUM']    | [3.1, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.11 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Under specific condition an unauthorised project member was allowed to delete a protected branches due to a business logic error.  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-39932 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Using large payloads, the diff feature could be used to trigger high load time for users reviewing code changes.                                      |
| Git | 2.45.2 | CVE-2021-39933 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.10 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. A regular expression used for handling user input (notes, comments, etc) was susceptible to catastrophic backtracking that could cause a DOS attack. |
| Git | 2.45.2 | CVE-2021-39934 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper access control allows any project member to retrieve the service desk email address in GitLab CE/EE versions starting 12.10 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2.   |
| Git | 2.45.2 | CVE-2021-39935 | ['MEDIUM', 'HIGH']   | [6.8, 7.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.5 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Unauthorized external users could perform Server Side Requests via the CI Lint API  |
| Git | 2.45.2 | CVE-2021-39936 | ['LOW', 'MEDIUM']    | [3.5, 4.3] | Improper access control in GitLab CE/EE affecting all versions starting from 10.7 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker in possession of a deploy token to access a project's disabled wiki.  |
| Git | 2.45.2 | CVE-2021-39937 | ['MEDIUM', 'HIGH']   | [5.9, 8.8] | A collision in access memoization logic in all versions of GitLab CE/EE before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, leads to potential elevated privileges in groups and projects under rare circumstances   |
| Git | 2.45.2 | CVE-2021-39938 | ['LOW', 'MEDIUM']    | [3.1, 6.5] | A vulnerable regular expression pattern in GitLab CE/EE since version 8.15 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker to cause uncontrolled resource consumption leading to Denial of Service via specially crafted deploy Slash commands                            |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-39939 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An uncontrolled resource consumption vulnerability in GitLab Runner affecting all versions starting from 13.7 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an attacker triggering a job with a specially crafted docker image to exhaust resources on runner manager                                   |
| Git | 2.45.2 | CVE-2021-39940 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.2 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. GitLab Maven Package registry is vulnerable to a regular expression denial of service when a specifically crafted string is sent.   |
| Git | 2.45.2 | CVE-2021-39941 | ['LOW', 'MEDIUM']    | [3.7, 5.3] | An information disclosure vulnerability in GitLab CE/EE versions 12.0 to 14.3.6, 14.4 to 14.4.4, and 14.5 to 14.5.2 allowed non-project members to see the default branch name for projects that restrict access to the repository to project members   |
| Git | 2.45.2 | CVE-2021-39944 | ['HIGH', 'HIGH']     | [7.1, 7.1] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. A permissions validation flaw allowed group members with a developer role to elevate their privilege to a maintainer on projects they import                              |
| Git | 2.45.2 | CVE-2021-39945 | ['LOW', 'LOW']       | [2.7, 2.7] | Improper access control in the GitLab CE/EE API affecting all versions starting from 9.4 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows an author of a Merge Request to approve the Merge Request even after having their project access revoked   |
| Git | 2.45.2 | CVE-2021-34426 | ['MEDIUM', 'HIGH']   | [5.3, 7.8] | A vulnerability was discovered in the Keybase Client for Windows before version 5.6.0 when a user executed the "keybase git lfs-config" command on the command-line. In versions prior to 5.6.0, a malicious actor with write access to a user's Git repository could leverage this vulnerability to potentially execute arbitrary Windows commands on a user's local system. |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-43846 | ['MEDIUM', 'MEDIUM'] | [5.3, 4.3] | <code>`solidus_frontend`</code> is the cart and storefront for the Solidus e-commerce project. Versions of <code>`solidus_frontend`</code> prior to 3.1.5, 3.0.5, and 2.11.14 contain a cross-site request forgery (CSRF) vulnerability that allows a malicious site to add an item to the user's cart without their knowledge. Versions 3.1.5, 3.0.5, and 2.11.14 contain a patch for this issue. The patch adds CSRF token verification to the "Add to cart" action. Adding forgery protection to a form that missed it can have some side effects. Other CSRF protection strategies as well as a workaround involving modification to <code>config/application.rb`</code> are available. More details on these mitigations are available in the GitHub Security Advisory.  |
| Git | 2.45.2 | CVE-2021-23772 | ['HIGH', 'HIGH']     | [7.5, 8.8] | This affects all versions of package <code>github.com/kataras/iris</code> ; all versions of package <code>github.com/kataras/iris/v12</code> . The unsafe handling of file names during upload using <code>UploadFormFiles</code> method may enable attackers to write to arbitrary locations outside the designated target folder.   |
| Git | 2.45.2 | CVE-2021-43862 | ['LOW', 'MEDIUM']    | [3.7, 5.4] | jQuery Terminal Emulator is a plugin for creating command line interpreters in your applications. Versions prior to 2.31.1 contain a low impact and limited cross-site scripting (XSS) vulnerability. The code for XSS payload is always visible, but an attacker can use other techniques to hide the code the victim sees. If the application uses the <code>`execHash`</code> option and executes code from URL, the attacker can use this URL to execute their code. The scope is limited because the javascript attribute used is added to span tag, so no automatic execution like with <code>`onerror`</code> on images is possible. This issue is fixed in version 2.31.1. As a workaround, the user can use formatting that wrap whole user input and its no op. The code for this workaround is available in the GitHub Security Advisory. The fix will only work when user of the library is not using different formatters (e.g. to highlight code in different way). |
| Git | 2.45.2 | CVE-2020-23986 | MEDIUM               | 6.1        | Github Read Me Stats commit <code>3c7220e4f7144f6cb068fd433c774f6db47ccb95</code> was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the function <code>renderError</code> .  |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-21668 | ['HIGH', 'HIGH']   | [8.0, 8.6] | <p>pipenv is a Python development workflow tool. Starting with version 2018.10.9 and prior to version 2022.1.8, a flaw in pipenv's parsing of requirements files allows an attacker to insert a specially crafted string inside a comment anywhere within a requirements.txt file, which will cause victims who use pipenv to install the requirements file to download dependencies from a package index server controlled by the attacker. By embedding malicious code in packages served from their malicious index server, the attacker can trigger arbitrary remote code execution (RCE) on the victims' systems. If an attacker is able to hide a malicious '--index-url' option in a requirements file that a victim installs with pipenv, the attacker can embed arbitrary malicious code in packages served from their malicious index server that will be executed on the victim's host during installation (remote code execution/RCE). When pip installs from a source distribution, any code in the setup.py is executed by...</p> |
| Git | 2.45.2 | CVE-2022-21671 | ['HIGH', 'MEDIUM'] | [8.1, 6.5] | <p>@replit/crosis is a JavaScript client that speaks Replit's container protocol. A vulnerability that involves exposure of sensitive information exists in versions prior to 7.3.1. When using this library as a way to programmatically communicate with Replit in a standalone fashion, if there are multiple failed attempts to contact Replit through a WebSocket, the library will attempt to communicate using a fallback poll-based proxy. The URL of the proxy has changed, so any communication done to the previous URL could potentially reach a server that is outside of Replit's control and the token used to connect to the Repl could be obtained by an attacker, leading to full compromise of that Repl (not of the account). This was patched in version 7.3.1 by updating the address of the fallback WebSocket polling proxy to the new one. As a workaround, a user may specify the new address for the polling host ('gp-v2.replit.com') in the 'ConnectArgs'. More information about this workaround is availa...</p> |
| Git | 2.45.2 | CVE-2022-0242  | HIGH               | 7.2        | <p>Unrestricted Upload of File with Dangerous Type in GitHub repository crater-invoice/crater prior to 6.0.</p>   |
| Git | 2.45.2 | CVE-2022-0245  | MEDIUM             | 4.3        | <p>Cross-Site Request Forgery (CSRF) in GitHub repository livehelperchat/livehelperchat prior to 2.0.</p>   |
| Git | 2.45.2 | CVE-2022-0260  | MEDIUM             | 5.4        | <p>Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.2.7.</p>  |
| Git | 2.45.2 | CVE-2021-4146  | MEDIUM             | 4.3        | <p>Business Logic Errors in GitHub repository pimcore/pimcore prior to 10.2.6.</p>  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-0261  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2021-39892 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE since version 12.0, a lower privileged user can import users from projects that they don't have a maintainer role on and disclose email addresses of those users.   |
| Git | 2.45.2 | CVE-2021-39927 | ['LOW', 'MEDIUM']    | [3.5, 4.3] | Server side request forgery protections in GitLab CE/EE versions between 8.4 and 14.4.4, between 14.5.0 and 14.5.2, and between 14.6.0 and 14.6.1 would fail to protect against attacks sending requests to localhost on port 80 or 443 if GitLab was configured to run on a port other than 80 or 443                                |
| Git | 2.45.2 | CVE-2021-39942 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.5] | A denial of service vulnerability in GitLab CE/EE affecting all versions starting from 12.0 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allows low-privileged users to bypass file size limits in the NPM package repository to potentially cause denial of service. |
| Git | 2.45.2 | CVE-2021-39946 | ['HIGH', 'MEDIUM']   | [8.7, 5.4] | Improper neutralization of user input in GitLab CE/EE versions 14.3 to 14.3.6, 14.4 to 14.4.4, and 14.5 to 14.5.2 allowed an attacker to exploit XSS by abusing the generation of the HTML code related to emojis   |
| Git | 2.45.2 | CVE-2022-0090  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab is configured in a way that it doesn't ignore replacement references with git sub-commands, allowing a malicious user to spoof the contents of their commits in the UI.                      |
| Git | 2.45.2 | CVE-2022-0093  | ['LOW', 'MEDIUM']    | [3.5, 4.3] | An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab allows a user with an expired password to access sensitive information through RSS feeds.  |
| Git | 2.45.2 | CVE-2022-0124  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. Gitlab's Slack integration is incorrectly validating user input and allows to craft malicious URLs that are sent to slack.  |
| Git | 2.45.2 | CVE-2022-0125  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting all versions starting from 12.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not verifying that a maintainer of a project had the right access to import members from a target project.               |

|     |        |               |                      |            |  |
|-----|--------|---------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-0151 | ['MEDIUM', 'MEDIUM'] | [6.5, 4.9] | An issue has been discovered in GitLab affecting all versions starting from 12.10 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not correctly handling requests to delete existing packages which could result in a Denial of Service under specific conditions.                   |
| Git | 2.45.2 | CVE-2022-0152 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An issue has been discovered in GitLab affecting all versions starting from 13.10 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to unauthorized access to some particular fields through the GraphQL API.   |
| Git | 2.45.2 | CVE-2022-0154 | ['HIGH', 'HIGH']     | [7.5, 8.0] | An issue has been discovered in GitLab affecting all versions starting from 7.7 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to a Cross-Site Request Forgery attack that allows a malicious user to have their GitHub project imported on another GitLab user account. |
| Git | 2.45.2 | CVE-2022-0172 | ['MEDIUM', 'MEDIUM'] | [5.3, 6.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.3. Under certain conditions it was possible to bypass the IP restriction for public projects through GraphQL allowing unauthorised users to read titles of issues, merge requests and milestones.   |
| Git | 2.45.2 | CVE-2022-0244 | ['HIGH', 'HIGH']     | [8.6, 7.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting with 14.5. Arbitrary file read was possible by importing a group was due to incorrect handling of file.   |
| Git | 2.45.2 | CVE-2021-4143 | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Generic in GitHub repository bigbluebutton/bigbluebutton prior to 2.4.0.  |
| Git | 2.45.2 | CVE-2021-3866 | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository zulip/zulip more than and including 44f935695d452cc3fb16845a0c6af710438b153d and prior to 3eb2791c3e9695f7d37ffe84e0c2184fae665cb6.   |
| Git | 2.45.2 | CVE-2022-0219 | MEDIUM               | 5.5        | Improper Restriction of XML External Entity Reference in GitHub repository skylot/jadx prior to 1.3.2.   |
| Git | 2.45.2 | CVE-2021-4172 | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository star7th/showdoc prior to 2.10.2.  |
| Git | 2.45.2 | CVE-2021-4103 | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository vanessa219/vditor prior to 1.0.34.  |
| Git | 2.45.2 | CVE-2021-3850 | CRITICAL             | 9.1        | Authentication Bypass by Primary Weakness in GitHub repository adodb/adodb prior to 5.20.21.   |

|     |        |                |        |     |  |
|-----|--------|----------------|--------|-----|--|
| Git | 2.45.2 | CVE-2022-0351  | HIGH   | 7.8 | Access of Memory Location Before Start of Buffer in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2021-41598 | HIGH   | 8.8 | A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more permissions to be granted during a GitHub App's user-authorization web flow than was displayed to the user during approval. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. All permissions being granted would properly be shown during the first authorization, but if the user later updated the set of repositories the app was installed on after the GitHub App had configured additional user-level permissions, those additional permissions would not be displayed, leading to more permissions being granted than the user potentially intended. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.2.5, 3.1.13, 3.0.21. This vulnerability was reported via the GitHub Bug Bounty program. |
| Git | 2.45.2 | CVE-2022-0251  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.2.10.   |
| Git | 2.45.2 | CVE-2022-0359  | HIGH   | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-0203  | MEDIUM | 5.3 | Improper Access Control in GitHub repository crater-invoice/crater prior to 6.0.2.   |
| Git | 2.45.2 | CVE-2022-0361  | HIGH   | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-0368  | HIGH   | 7.8 | Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-4160  | MEDIUM               | 5.9        | There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. F... |
| Git | 2.45.2 | CVE-2022-0392  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-0393  | HIGH                 | 7.1        | Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-23598 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | laminas-form is a package for validating and displaying simple and complex forms. When rendering validation error messages via the `formElementErrors()` view helper shipped with laminas-form, many messages will contain the submitted value. However, in laminas-form prior to version 3.1.1, the value was not being escaped for HTML contexts, which could potentially lead to a reflected cross-site scripting attack. Versions 3.1.1 and above contain a patch to mitigate the vulnerability. A workaround is available. One may manually place code at the top of a view script where one calls the `formElementErrors()` view helper. More information about this workaround is available on the GitHub Security Advisory.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-23599 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.1] | Products.ATContentTypes are the core content types for Plone 2.1 - 4.3. Versions of Plone that are dependent on Products.ATContentTypes prior to version 3.0.6 are vulnerable to reflected cross site scripting and open redirect when an attacker can get a compromised version of the image_view_fullscreen page in a cache, for example in Varnish. The technique is known as cache poisoning. Any later visitor can get redirected when clicking on a link on this page. Usually only anonymous users are affected, but this depends on the user's cache settings. Version 3.0.6 of Products.ATContentTypes has been released with a fix. This version works on Plone 5.2, Python 2 only. As a workaround, make sure the image_view_fullscreen page is not stored in the cache. More information about the vulnerability and cvmitigation measures is available in the GitHub Security Advisory. |
| Git | 2.45.2 | CVE-2022-0407  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-0408  | HIGH                 | 7.8        | Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-0413  | HIGH                 | 7.8        | Use After Free in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2021-46101 | HIGH                 | 7.5        | In Git for windows through 2.34.1 when using git pull to update the local warehouse, git.cmd can be run directly.  |
| Git | 2.45.2 | CVE-2022-0419  | MEDIUM               | 5.5        | NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.0.  |
| Git | 2.45.2 | CVE-2022-0417  | HIGH                 | 7.8        | Heap-based Buffer Overflow GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-0443  | HIGH                 | 7.8        | Use After Free in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-0432  | MEDIUM               | 6.1        | Prototype Pollution in GitHub repository mastodon/mastodon prior to 3.5.0.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-23569 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Tensorflow is an Open Source Machine Learning Framework. Multiple operations in TensorFlow can be used to trigger a denial of service via `CHECK`-fails (i.e., assertion failures). This is similar to TFSA-2021-198 and has similar fixes. We have patched the reported issues in multiple GitHub commits. It is possible that other similar instances exist in TensorFlow, we will issue fixes as these are discovered. The fix will be included in TensorFlow 2.8.0. We will also cherry-pick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. |
| Git | 2.45.2 | CVE-2021-45429 | MEDIUM               | 5.5        | A Buffer Overflow vulnerability exists in VirusTotal YARA git commit: 605b2edf07ed8eb9a2c61ba22eb2e7c362f47ba7 via yr_set_configuration in yara/libyara/libyara.c, which could cause a Denial of Service.  |
| Git | 2.45.2 | CVE-2021-4043  | MEDIUM               | 5.5        | NULL Pointer Dereference in GitHub repository gpac/gpac prior to 1.1.0.  |
| Git | 2.45.2 | CVE-2022-23590 | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | Tensorflow is an Open Source Machine Learning Framework. A `GraphDef` from a TensorFlow `SavedModel` can be maliciously altered to cause a TensorFlow process to crash due to encountering a `StatusOr` value that is an error and forcibly extracting the value from it. We have patched the issue in multiple GitHub commits and these will be included in TensorFlow 2.8.0 and TensorFlow 2.7.1, as both are affected.  |
| Git | 2.45.2 | CVE-2022-0508  | MEDIUM               | 5.3        | Server-Side Request Forgery (SSRF) in GitHub repository chocobozzz/peertube prior to f33e515991a32885622b217bf2ed1d1b0d9d6832  |
| Git | 2.45.2 | CVE-2021-45325 | HIGH                 | 7.5        | Server Side Request Forgery (SSRF) vulnerability exists in Gitea before 1.7.0 using the OpenID URL.  |
| Git | 2.45.2 | CVE-2021-45326 | HIGH                 | 8.8        | Cross Site Request Forgery (CSRF) vulnerability exists in Gitea before 1.5.2 via API routes. This can be dangerous especially with state altering POST requests.   |
| Git | 2.45.2 | CVE-2021-45327 | CRITICAL             | 9.8        | Gitea before 1.11.2 is affected by Trusting HTTP Permission Methods on the Server Side when referencing the vulnerable admin or user API, which could let a remote malicious user execute arbitrary code.  |
| Git | 2.45.2 | CVE-2021-45328 | MEDIUM               | 6.1        | Gitea before 1.4.3 is affected by URL Redirection to Untrusted Site ('Open Redirect') via internal URLs.   |
| Git | 2.45.2 | CVE-2022-0139  | CRITICAL             | 9.8        | Use After Free in GitHub repository radareorg/radare2 prior to 5.6.0.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-0518  | HIGH                 | 7.1        | Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.2.  |
| Git | 2.45.2 | CVE-2022-0519  | HIGH                 | 7.1        | Buffer Access with Incorrect Length Value in GitHub repository radareorg/radare2 prior to 5.6.2.   |
| Git | 2.45.2 | CVE-2022-0521  | HIGH                 | 7.1        | Access of Memory Location After End of Buffer in GitHub repository radareorg/radare2 prior to 5.6.2.   |
| Git | 2.45.2 | CVE-2022-0523  | HIGH                 | 7.8        | Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2.  |
| Git | 2.45.2 | CVE-2022-0524  | HIGH                 | 7.5        | Business Logic Errors in GitHub repository publiify/publify prior to 9.2.7.  |
| Git | 2.45.2 | CVE-2021-45329 | MEDIUM               | 6.1        | Cross Site Scripting (XSS) vulnerability exists in Gitea before 1.5.1 via the repository settings inside the external wiki/issue tracker URL field.  |
| Git | 2.45.2 | CVE-2022-0526  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0.   |
| Git | 2.45.2 | CVE-2022-0527  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0.   |
| Git | 2.45.2 | CVE-2021-3813  | MEDIUM               | 6.5        | Improper Privilege Management in GitHub repository chatwoot/chatwoot prior to v2.2.  |
| Git | 2.45.2 | CVE-2021-45330 | CRITICAL             | 9.8        | An issue exists in Gitea through 1.15.7, which could let a malicious user gain privileges due to client side cookies not being deleted and the session remains valid on the server side for reuse.   |
| Git | 2.45.2 | CVE-2021-45331 | CRITICAL             | 9.8        | An Authentication Bypass vulnerability exists in Gitea before 1.5.0, which could let a malicious user gain privileges. If captured, the TOTP code for the 2FA can be submitted correctly more than once.   |
| Git | 2.45.2 | CVE-2021-39943 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An authorization logic error in the External Status Check API in GitLab EE affecting all versions starting from 14.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allowed a user to update the status of the check via an API call   |
| Git | 2.45.2 | CVE-2022-0554  | HIGH                 | 7.8        | Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-24975 | HIGH                 | 7.5        | The --mirror documentation for Git through 2.35.1 does not mention the availability of deleted content, aka the "GitBleed" issue. This could present a security risk if information-disclosure auditing processes rely on a clone operation without the --mirror option. Note: This has been disputed by multiple 3rd parties who believe this is an intended feature of the git binary and does not pose a security risk. |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-0571  | MEDIUM             | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository phoronix-test-suite/phoronix-test-suite prior to 10.8.2.   |
| Git | 2.45.2 | CVE-2022-0572  | HIGH               | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-25196 | MEDIUM             | 5.4        | Jenkins GitLab Authentication Plugin 1.13 and earlier records the HTTP Referer header as part of the URL query parameters when the authentication process starts, allowing attackers with access to Jenkins to craft a URL that will redirect users to an attacker-specified URL after logging in.   |
| Git | 2.45.2 | CVE-2022-0559  | CRITICAL           | 9.8        | Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2.  |
| Git | 2.45.2 | CVE-2022-23636 | ['MEDIUM', 'HIGH'] | [5.1, 8.1] | Wasmtime is an open source runtime for WebAssembly & WASI. Prior to versions 0.34.1 and 0.33.1, there exists a bug in the pooling instance allocator in Wasmtime's runtime where a failure to instantiate an instance for a module that defines an `externref` global will result in an invalid drop of a `VMExternRef` via an uninitialized pointer. A number of conditions listed in the GitHub Security Advisory must be true in order for an instance to be vulnerable to this issue. Maintainers believe that the effective impact of this bug is relatively small because the usage of `externref` is still uncommon and without a resource limiter configured on the `Store`, which is not the default configuration, it is only possible to trigger the bug from an error returned by `mprotect` or `VirtualAlloc`. Note that on Linux with the `uffd` feature enabled, it is only possible to trigger the bug from a resource limiter as the call to `mprotect` is skipped. The bug has been fixed in 0.34.1 and 0.33.1 and ... |
| Git | 2.45.2 | CVE-2022-0629  | HIGH               | 7.8        | Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2021-41599 | HIGH               | 8.8        | A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.0.21, 3.1.13, 3.2.5. This vulnerability was reported via the GitHub Bug Bounty program.   |
| Git | 2.45.2 | CVE-2022-0664  | CRITICAL           | 9.8        | Use of Hard-coded Cryptographic Key in Go github.com/gravitl/netmaker prior to 0.8.5,0.9.4,0.10.0,0.10.1.  |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2022-23642 | ['HIGH', 'HIGH'] | [8.8, 8.8] | Sourcegraph is a code search and navigation engine. Sourcegraph prior to version 3.37 is vulnerable to remote code execution in the `gitserver` service. The service acts as a git exec proxy, and fails to properly restrict calling `git config`. This allows an attacker to set the git `core.sshCommand` option, which sets git to use the specified command instead of ssh when they need to connect to a remote system. Exploitation of this vulnerability depends on how Sourcegraph is deployed. An attacker able to make HTTP requests to internal services like gitserver is able to exploit it. This issue is patched in Sourcegraph version 3.37. As a workaround, ensure that requests to gitserver are properly protected. |
| Git | 2.45.2 | CVE-2022-0685  | HIGH             | 7.8        | Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4418.   |
| Git | 2.45.2 | CVE-2022-0696  | MEDIUM           | 5.5        | NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.4428.   |
| Git | 2.45.2 | CVE-2022-0676  | HIGH             | 7.8        | Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.4.  |
| Git | 2.45.2 | CVE-2022-0665  | MEDIUM           | 6.5        | Path Traversal in GitHub repository pimcore/pimcore prior to 10.3.2.   |
| Git | 2.45.2 | CVE-2022-0712  | MEDIUM           | 5.5        | NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.4.  |
| Git | 2.45.2 | CVE-2022-0713  | HIGH             | 7.1        | Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.4.  |
| Git | 2.45.2 | CVE-2022-0714  | MEDIUM           | 5.5        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.4436.   |
| Git | 2.45.2 | CVE-2022-0654  | HIGH             | 7.5        | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository fgribreau/node-request-retry prior to 7.0.0.   |
| Git | 2.45.2 | CVE-2022-0717  | CRITICAL         | 9.1        | Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2.  |
| Git | 2.45.2 | CVE-2022-0736  | HIGH             | 7.5        | Insecure Temporary File in GitHub repository mlflow/mlflow prior to 1.23.1.  |
| Git | 2.45.2 | CVE-2022-0719  | MEDIUM           | 5.4        | Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3.  |
| Git | 2.45.2 | CVE-2022-0721  | MEDIUM           | 6.5        | Insertion of Sensitive Information Into Debugging Code in GitHub repository microweber/microweber prior to 1.3.  |
| Git | 2.45.2 | CVE-2022-0724  | MEDIUM           | 6.5        | Insecure Storage of Sensitive Information in GitHub repository microweber/microweber prior to 1.3.   |
| Git | 2.45.2 | CVE-2022-0726  | MEDIUM           | 5.4        | Missing Authorization in GitHub repository chocobozzz/peertube prior to 4.1.0.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-0727  | MEDIUM               | 5.4        | Improper Access Control in GitHub repository chocobozzz/peertube prior to 4.1.0.   |
| Git | 2.45.2 | CVE-2022-0729  | HIGH                 | 8.8        | Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440.   |
| Git | 2.45.2 | CVE-2022-0476  | MEDIUM               | 5.5        | Denial of Service in GitHub repository radareorg/radare2 prior to 5.6.4.   |
| Git | 2.45.2 | CVE-2022-0731  | MEDIUM               | 6.5        | Improper Access Control (IDOR) in GitHub repository dolibarr/dolibarr prior to 16.0.   |
| Git | 2.45.2 | CVE-2021-4070  | CRITICAL             | 9.1        | Off-by-one Error in GitHub repository v2fly/v2ray-core prior to 4.44.0.  |
| Git | 2.45.2 | CVE-2022-0695  | MEDIUM               | 5.5        | Denial of Service in GitHub repository radareorg/radare2 prior to 5.6.4.   |
| Git | 2.45.2 | CVE-2022-0746  | MEDIUM               | 4.3        | Business Logic Errors in GitHub repository dolibarr/dolibarr prior to 16.0.  |
| Git | 2.45.2 | CVE-2022-24331 | CRITICAL             | 9.8        | In JetBrains TeamCity before 2021.1.4, GitLab authentication impersonation was possible.   |
| Git | 2.45.2 | CVE-2022-0762  | ['MEDIUM', 'MEDIUM'] | [5.5, 4.3] | Incorrect Authorization in GitHub repository microweber/microweber prior to 1.3.   |
| Git | 2.45.2 | CVE-2022-0763  | MEDIUM               | 4.8        | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.   |
| Git | 2.45.2 | CVE-2022-0723  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.11.   |
| Git | 2.45.2 | CVE-2022-0764  | MEDIUM               | 6.7        | Arbitrary Command Injection in GitHub repository strapi/strapi prior to 4.1.0.   |
| Git | 2.45.2 | CVE-2021-3967  | HIGH                 | 8.8        | Improper Access Control in GitHub repository zulip/zulip prior to 4.10.  |
| Git | 2.45.2 | CVE-2022-0772  | MEDIUM               | 4.8        | Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.2.2.  |
| Git | 2.45.2 | CVE-2022-0768  | CRITICAL             | 9.1        | Server-Side Request Forgery (SSRF) in GitHub repository rudloff/alltube prior to 3.0.2.  |
| Git | 2.45.2 | CVE-2022-0743  | MEDIUM               | 4.6        | Cross-site Scripting (XSS) - Stored in GitHub repository getgrav/grav prior to 1.7.31.   |
| Git | 2.45.2 | CVE-2022-0776  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - DOM in GitHub repository hakimel/reveal.js prior to 4.3.0.  |
| Git | 2.45.2 | CVE-2022-0777  | HIGH                 | 7.5        | Weak Password Recovery Mechanism for Forgotten Password in GitHub repository microweber/microweber prior to 1.3.                                     |
| Git | 2.45.2 | CVE-2021-45860 | MEDIUM               | 5.5        | An integer overflow in DTSSStreamReader::findFrame () of tsMuxer git-2678966 allows attackers to cause a Denial of Service (DoS) via a crafted file. |
| Git | 2.45.2 | CVE-2021-45861 | MEDIUM               | 5.5        | There is an Assertion `num <= INT_BIT' failed at BitStreamReader::skipBits in /bitStream.h:132 of tsMuxer git-c6a0277.                               |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2021-45863 | MEDIUM               | 5.5        | tsMuxer git-2678966 was discovered to contain a heap-based buffer overflow via the function HevcUnit::updateBits in hevc.cpp.   |
| Git | 2.45.2 | CVE-2021-45864 | MEDIUM               | 5.5        | tsMuxer git-c6a0277 was discovered to contain a segmentation fault via DTSSStreamReader::findFrame in dtsStreamReader.cpp.  |
| Git | 2.45.2 | CVE-2022-0577  | MEDIUM               | 6.5        | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository scrapy/scrapy prior to 2.6.1.   |
| Git | 2.45.2 | CVE-2022-0824  | HIGH                 | 8.8        | Improper Access Control to Remote Code Execution in GitHub repository webmin/webmin prior to 1.990.   |
| Git | 2.45.2 | CVE-2022-0829  | HIGH                 | 8.1        | Improper Authorization in GitHub repository webmin/webmin prior to 1.990.   |
| Git | 2.45.2 | CVE-2022-0819  | HIGH                 | 8.8        | Code Injection in GitHub repository dolibarr/dolibarr prior to 15.0.1.  |
| Git | 2.45.2 | CVE-2022-0528  | ['MEDIUM', 'HIGH']   | [6.5, 7.5] | Server-Side Request Forgery (SSRF) in GitHub repository transloadit/uppy prior to 3.3.1.  |
| Git | 2.45.2 | CVE-2022-0753  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.5.9.   |
| Git | 2.45.2 | CVE-2022-0841  | CRITICAL             | 9.8        | OS Command Injection in GitHub repository ljharp/npm-lockfile in v2.0.3 and v2.0.4.   |
| Git | 2.45.2 | CVE-2022-24724 | ['HIGH', 'CRITICAL'] | [8.8, 9.8] | cmark-gfm is GitHub's extended version of the C reference implementation of CommonMark. Prior to versions 0.29.0.gfm.3 and 0.28.3.gfm.21, an integer overflow in cmark-gfm's table row parsing `table.c:row_from_string` may lead to heap memory corruption when parsing tables who's marker rows contain more than UINT16_MAX columns. The impact of this heap corruption ranges from Information Leak to Arbitrary Code Execution depending on how and where `cmark-gfm` is used. If `cmark-gfm` is used for rendering remote user controlled markdown, this vulnerability may lead to Remote Code Execution (RCE) in applications employing affected versions of the `cmark-gfm` library. This vulnerability has been patched in the following cmark-gfm versions 0.29.0.gfm.3 and 0.28.3.gfm.21. A workaround is available. The vulnerability exists in the table markdown extensions of cmark-gfm. Disabling the table extension will prevent this vulnerability from being triggered. |
| Git | 2.45.2 | CVE-2022-0265  | CRITICAL             | 9.8        | Improper Restriction of XML External Entity Reference in GitHub repository hazelcast/hazelcast in 5.1-BETA-1.   |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2022-0838  | MEDIUM           | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.5.10.  |
| Git | 2.45.2 | CVE-2022-0848  | CRITICAL         | 9.8        | OS Command Injection in GitHub repository part-db/part-db prior to 0.5.11.  |
| Git | 2.45.2 | CVE-2022-0752  | MEDIUM           | 6.1        | Cross-site Scripting (XSS) - Generic in GitHub repository hestiacp/hestiacp prior to 1.5.9.   |
| Git | 2.45.2 | CVE-2022-0831  | MEDIUM           | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3.   |
| Git | 2.45.2 | CVE-2022-0832  | MEDIUM           | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3.   |
| Git | 2.45.2 | CVE-2022-0839  | CRITICAL         | 9.8        | Improper Restriction of XML External Entity Reference in GitHub repository liquibase/liquibase prior to 4.8.0.  |
| Git | 2.45.2 | CVE-2022-0855  | MEDIUM           | 6.1        | Improper Resolution of Path Equivalence in GitHub repository microweber-dev/whmcs_plugin prior to 0.0.4.  |
| Git | 2.45.2 | CVE-2022-23915 | ['HIGH', 'HIGH'] | [7.2, 8.8] | The package weblate from 0 and before 4.11.1 are vulnerable to Remote Code Execution (RCE) via argument injection when using git or mercurial repositories. Authenticated users, can change the behavior of the application in an unintended way, leading to command execution. |
| Git | 2.45.2 | CVE-2022-0849  | MEDIUM           | 5.5        | Use After Free in r_reg_get_name_idx in GitHub repository radareorg/radare2 prior to 5.6.6.   |
| Git | 2.45.2 | CVE-2022-0845  | CRITICAL         | 9.8        | Code Injection in GitHub repository pytorchlightning/pytorch-lightning prior to 1.6.0.  |
| Git | 2.45.2 | CVE-2022-0869  | MEDIUM           | 6.1        | Multiple Open Redirect in GitHub repository nitely/spirit prior to 0.12.3.  |
| Git | 2.45.2 | CVE-2022-0868  | MEDIUM           | 6.1        | Open Redirect in GitHub repository medialize/uri.js prior to 1.19.10.   |
| Git | 2.45.2 | CVE-2022-0697  | MEDIUM           | 6.1        | Open Redirect in GitHub repository archivy/archivy prior to 1.7.0.  |
| Git | 2.45.2 | CVE-2022-0766  | CRITICAL         | 9.8        | Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.17.   |
| Git | 2.45.2 | CVE-2022-0767  | CRITICAL         | 9.9        | Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.17.   |
| Git | 2.45.2 | CVE-2022-0754  | MEDIUM           | 6.5        | SQL Injection in GitHub repository salesagility/suitecrm prior to 7.12.5.   |
| Git | 2.45.2 | CVE-2022-0755  | MEDIUM           | 4.3        | Missing Authorization in GitHub repository salesagility/suitecrm prior to 7.12.5.   |
| Git | 2.45.2 | CVE-2022-0756  | MEDIUM           | 6.5        | Missing Authorization in GitHub repository salesagility/suitecrm prior to 7.12.5.   |

|     |        |               |          |     |   |
|-----|--------|---------------|----------|-----|---|
| Git | 2.45.2 | CVE-2022-0877 | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository bookstackapp/bookstack prior to v22.02.3.                                    |
| Git | 2.45.2 | CVE-2022-0881 | MEDIUM   | 6.5 | Insecure Storage of Sensitive Information in GitHub repository chocobozzz/peertube prior to 4.1.1.                                    |
| Git | 2.45.2 | CVE-2022-0482 | CRITICAL | 9.1 | Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository alexselegidis/easyappointments prior to 1.4.3. |
| Git | 2.45.2 | CVE-2022-0896 | HIGH     | 8.8 | Improper Neutralization of Special Elements Used in a Template Engine in GitHub repository microweber/microweber prior to 1.3.        |
| Git | 2.45.2 | CVE-2022-0890 | MEDIUM   | 5.5 | NULL Pointer Dereference in GitHub repository mruby/mruby prior to 3.2.   |
| Git | 2.45.2 | CVE-2022-0895 | CRITICAL | 9.8 | Static Code Injection in GitHub repository microweber/microweber prior to 1.3.  |
| Git | 2.45.2 | CVE-2022-0905 | HIGH     | 7.1 | Missing Authorization in GitHub repository go-gitea/gitea prior to 1.16.4.  |
| Git | 2.45.2 | CVE-2022-0906 | MEDIUM   | 4.8 | Unrestricted file upload leads to stored XSS in GitHub repository microweber/microweber prior to 1.1.12.                              |
| Git | 2.45.2 | CVE-2022-0820 | MEDIUM   | 6.1 | Cross-site Scripting (XSS) - Stored in GitHub repository orchardcms/orchardcore prior to 1.3.0.                                       |
| Git | 2.45.2 | CVE-2022-0821 | MEDIUM   | 6.5 | Improper Authorization in GitHub repository orchardcms/orchardcore prior to 1.3.0.  |
| Git | 2.45.2 | CVE-2022-0822 | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - Reflected in GitHub repository orchardcms/orchardcore prior to 1.3.0.                                    |
| Git | 2.45.2 | CVE-2022-0912 | MEDIUM   | 4.8 | Unrestricted Upload of File with Dangerous Type in GitHub repository microweber/microweber prior to 1.2.11.                           |
| Git | 2.45.2 | CVE-2022-0913 | HIGH     | 7.5 | Integer Overflow or Wraparound in GitHub repository microweber/microweber prior to 1.3.   |
| Git | 2.45.2 | CVE-2022-0870 | MEDIUM   | 5.3 | Server-Side Request Forgery (SSRF) in GitHub repository gogs/gogs prior to 0.12.5.  |
| Git | 2.45.2 | CVE-2022-0928 | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.12.                                       |
| Git | 2.45.2 | CVE-2022-0871 | CRITICAL | 9.1 | Missing Authorization in GitHub repository gogs/gogs prior to 0.12.5.   |
| Git | 2.45.2 | CVE-2022-0860 | CRITICAL | 9.1 | Improper Authorization in GitHub repository cobbler/cobbler prior to 3.3.2.   |
| Git | 2.45.2 | CVE-2022-0932 | MEDIUM   | 6.5 | Missing Authorization in GitHub repository saleor/saleor prior to 3.1.2.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-24433 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package simple-git before 3.3.0 are vulnerable to Command Injection via argument injection. When calling the .fetch(remote, branch, handlerFn) function, both the remote and branch parameters are passed to the git fetch subcommand. By injecting some git options it was possible to get arbitrary command execution. |
| Git | 2.45.2 | CVE-2022-0921  | MEDIUM               | 6.7        | Abusing Backup/Restore feature to achieve Remote Code Execution in GitHub repository microweber/microweber prior to 1.2.12.  |
| Git | 2.45.2 | CVE-2022-0880  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository star7th/showdoc prior to 2.10.2.  |
| Git | 2.45.2 | CVE-2022-0926  | MEDIUM               | 4.8        | File upload filter bypass leading to stored XSS in GitHub repository microweber/microweber prior to 1.2.12.  |
| Git | 2.45.2 | CVE-2022-0929  | MEDIUM               | 6.1        | XSS on dynamic_text module in GitHub repository microweber/microweber prior to 1.2.11.   |
| Git | 2.45.2 | CVE-2022-0930  | MEDIUM               | 4.8        | File upload filter bypass leading to stored XSS in GitHub repository microweber/microweber prior to 1.2.12.  |
| Git | 2.45.2 | CVE-2022-0937  | MEDIUM               | 5.4        | Stored xss in showdoc through file upload in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0341  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository vanessa219/vditor prior to 3.8.12.  |
| Git | 2.45.2 | CVE-2022-0938  | MEDIUM               | 5.4        | Stored XSS via file upload in GitHub repository star7th/showdoc prior to v2.10.4.  |
| Git | 2.45.2 | CVE-2022-0940  | MEDIUM               | 5.4        | Stored XSS due to Unrestricted File Upload in GitHub repository star7th/showdoc prior to v2.10.4.  |
| Git | 2.45.2 | CVE-2022-0941  | MEDIUM               | 5.4        | Stored XSS due to Unrestricted File Upload in GitHub repository star7th/showdoc prior to v2.10.4.  |
| Git | 2.45.2 | CVE-2022-0946  | MEDIUM               | 5.4        | Stored XSS viva cshtml file upload in GitHub repository star7th/showdoc prior to v2.10.4.  |
| Git | 2.45.2 | CVE-2022-0960  | MEDIUM               | 5.4        | Stored XSS viva .properties file upload in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0962  | MEDIUM               | 5.4        | Stored XSS viva .webma file upload in GitHub repository star7th/showdoc prior to 2.10.4.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-20001 | ['HIGH', 'HIGH']     | [7.8, 7.8] | fish is a command line shell. fish version 3.1.0 through version 3.3.1 is vulnerable to arbitrary code execution. git repositories can contain per-repository configuration that change the behavior of git, including running arbitrary commands. When using the default configuration of fish, changing to a directory automatically runs `git` commands in order to display information about the current repository in the prompt. If an attacker can convince a user to change their current directory into one controlled by the attacker, such as on a shared file system or extracted archive, fish will run arbitrary commands under the attacker's control. This problem has been fixed in fish 3.4.0. Note that running git in these directories, including using the git tab completion, remains a potential trigger for this issue. As a workaround, remove the `fish_git_prompt` function from the prompt. |
| Git | 2.45.2 | CVE-2022-0943  | HIGH                 | 7.8        | Heap-based Buffer Overflow occurs in vim in GitHub repository vim/vim prior to 8.2.4563.   |
| Git | 2.45.2 | CVE-2022-24743 | ['HIGH', 'HIGH']     | [7.1, 8.2] | Sylus is an open source eCommerce platform. Prior to versions 1.10.11 and 1.11.2, the reset password token was not set to null after the password was changed. The same token could be used several times, which could result in leak of the existing token and unauthorized password change. The issue is fixed in versions 1.10.11 and 1.11.2. As a workaround, overwrite the `Sylus\Bundle\ApiBundle\CommandHandler\ResetPasswordHandler` class with code provided by the maintainers and register it in a container. More information about this workaround is available in the GitHub Security Advisory.  |
| Git | 2.45.2 | CVE-2022-24749 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | Sylus is an open source eCommerce platform. In versions prior to 1.9.10, 1.10.11, and 1.11.2, it is possible to upload an SVG file containing cross-site scripting (XSS) code in the admin panel. In order to perform a XSS attack, the file itself has to be open in a new card or loaded outside of the IMG tag. The problem applies both to the files opened on the admin panel and shop pages. The issue is fixed in versions 1.9.10, 1.10.11, and 1.11.2. As a workaround, require a library that adds on-upload file sanitization and overwrite the service before writing the file to the filesystem. The GitHub Security Advisory contains more specific information about the workaround.   |
| Git | 2.45.2 | CVE-2022-0944  | HIGH                 | 7.2        | Template injection in connection test endpoint leads to RCE in GitHub repository sqlpad/sqlpad prior to 6.10.1.  |

|     |        |                |                          |            |   |
|-----|--------|----------------|--------------------------|------------|---|
| Git | 2.45.2 | CVE-2022-0945  | MEDIUM                   | 5.4        | Stored XSS viva axd and cshtml file upload in star7th/showdoc in GitHub repository star7th/showdoc prior to v2.10.4.  |
| Git | 2.45.2 | CVE-2022-0950  | MEDIUM                   | 5.4        | Unrestricted Upload of File with Dangerous Type in GitHub repository star7th/showdoc prior to 2.10.4.   |
| Git | 2.45.2 | CVE-2022-0951  | MEDIUM                   | 6.1        | File Upload Restriction Bypass leading to Stored XSS Vulnerability in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0893  | MEDIUM                   | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.   |
| Git | 2.45.2 | CVE-2022-0894  | MEDIUM                   | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.   |
| Git | 2.45.2 | CVE-2022-0954  | MEDIUM                   | 5.4        | Multiple Stored Cross-site Scripting (XSS) Vulnerabilities in Shop's Other Settings, Shop's Autorespond E-mail Settings and Shops' Payments Methods in GitHub repository microweber/microweber prior to 1.2.11.   |
| Git | 2.45.2 | CVE-2022-0956  | MEDIUM                   | 5.4        | Stored XSS via File Upload in GitHub repository star7th/showdoc prior to v.2.10.4.  |
| Git | 2.45.2 | CVE-2022-0957  | MEDIUM                   | 5.4        | Stored XSS via File Upload in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0942  | MEDIUM                   | 5.4        | Stored XSS due to Unrestricted File Upload in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0430  | MEDIUM                   | 5.3        | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository httpie/httpie prior to 3.1.0.   |
| Git | 2.45.2 | CVE-2022-0961  | MEDIUM                   | 5.5        | The microweber application allows large characters to insert in the input field "post title" which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request. in GitHub repository microweber/microweber prior to 1.2.12.   |
| Git | 2.45.2 | CVE-2022-24752 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | SyllusGridBundle is a package of generic data grids for Symfony applications. Prior to versions 1.10.1 and 1.11-rc2, values added at the end of query sorting were passed directly to the database. The maintainers do not know if this could lead to direct SQL injections but took steps to remediate the vulnerability. The issue is fixed in versions 1.10.1 and 1.11-rc2. As a workaround, overwrite the `Syllus\Component\Grid\Sorting\Sorter.php` class and register it in the container. More information about this workaround is available in the GitHub Security Advisory. |
| Git | 2.45.2 | CVE-2022-0963  | MEDIUM                   | 5.4        | Unrestricted XML Files Leads to Stored XSS in GitHub repository microweber/microweber prior to 1.2.12.  |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2022-0964  | MEDIUM | 5.4 | Stored XSS viva .webmv file upload in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0965  | MEDIUM | 5.4 | Stored XSS viva .ofd file upload in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0966  | MEDIUM | 5.4 | Stored XSS via File Upload in star7th/showdoc in GitHub repository star7th/showdoc prior to 2.4.10.   |
| Git | 2.45.2 | CVE-2022-0967  | MEDIUM | 5.4 | Stored XSS via File Upload in star7th/showdoc in star7th/showdoc in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-0968  | MEDIUM | 5.5 | The microweber application allows large characters to insert in the input field "first & last name" which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request. in microweber/microweber in GitHub repository microweber/microweber prior to 1.2.12. |
| Git | 2.45.2 | CVE-2022-0970  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository getgrav/grav prior to 1.7.31.  |
| Git | 2.45.2 | CVE-2022-27206 | MEDIUM | 6.5 | Jenkins GitLab Authentication Plugin 1.13 and earlier stores the GitLab client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.                                      |
| Git | 2.45.2 | CVE-2022-27212 | MEDIUM | 5.4 | Jenkins List Git Branches Parameter Plugin 0.0.9 and earlier does not escape the name of the 'List Git branches (and more)' parameter, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.                    |
| Git | 2.45.2 | CVE-2021-29134 | MEDIUM | 5.3 | The avatar middleware in Gitea before 1.13.6 allows Directory Traversal via a crafted URL.  |
| Git | 2.45.2 | CVE-2022-0911  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.   |
| Git | 2.45.2 | CVE-2022-0704  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.   |
| Git | 2.45.2 | CVE-2022-0705  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.   |
| Git | 2.45.2 | CVE-2022-0986  | MEDIUM | 6.1 | Reflected Cross-site Scripting (XSS) Vulnerability in GitHub repository hestiacp/hestiacp prior to 1.5.11.  |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2022-23610 | ['CRITICAL', 'HIGH']   | [9.1, 8.1] | wire-server provides back end services for Wire, an open source messenger. In versions of wire-server prior to the 2022-01-27 release, it was possible to craft DSA Signatures to bypass SAML SSO and impersonate any Wire user with SAML credentials. In teams with SAML, but without SCIM, it was possible to create new accounts with fake SAML credentials. Under certain conditions that can be established by an attacker, an upstream library for parsing, rendering, signing, and validating SAML XML data was accepting public keys as trusted that were provided by the attacker in the signature. As a consequence, the attacker could login as any user in any Wire team with SAML SSO enabled. If SCIM was not enabled, the attacker could also create new users with new SAML NameIDs. In order to exploit this vulnerability, the attacker needs to know the SSO login code (distributed to all team members with SAML credentials and visible in the Team Management app), the SAML EntityID identifying the IdP (a U... |
| Git | 2.45.2 | CVE-2022-1000  | CRITICAL               | 9.8        | Path Traversal in GitHub repository prasathmani/tinyfilemanager prior to 2.4.7.  |
| Git | 2.45.2 | CVE-2021-23632 | ['MEDIUM', 'CRITICAL'] | [6.6, 9.8] | All versions of package git are vulnerable to Remote Code Execution (RCE) due to missing sanitization in the Git.git method, which allows execution of OS commands rather than just git commands. Steps to Reproduce 1. Create a file named exploit.js with the following content: <code>js var Git = require("git").Git; var repo = new Git("repo-test"); var user_input = "version; date"; repo.git(user_input, function(err, result) { console.log(result); })</code> 2. In the same directory as exploit.js, run <code>npm install git</code> . 3. Run <code>exploit.js: node exploit.js</code> . You should see the outputs of both the git version and date command-lines. Note that the repo-test Git repository does not need to be present to make this PoC work.   |
| Git | 2.45.2 | CVE-2022-21221 | ['MEDIUM', 'HIGH']     | [5.9, 7.5] | The package github.com/valyala/fasthttp before 1.34.0 are vulnerable to Directory Traversal via the ServeFile function, due to improper sanitization. It is possible to be exploited by using a backslash %5c character in the path. **Note:** This security issue impacts Windows users only.   |
| Git | 2.45.2 | CVE-2022-0991  | HIGH                   | 7.1        | Insufficient Session Expiration in GitHub repository admidio/admidio prior to 4.1.9.   |
| Git | 2.45.2 | CVE-2022-0415  | HIGH                   | 8.8        | Remote Command Execution in uploading repository file in GitHub repository gogs/gogs prior to 0.12.6.  |

|     |        |                |                   |            |  |
|-----|--------|----------------|-------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1035  | MEDIUM            | 5.5        | Segmentation Fault caused by MP4Box -lsr in GitHub repository gpac/gpac prior to 2.1.0-DEV.  |
| Git | 2.45.2 | CVE-2022-25766 | ['HIGH', 'HIGH']  | [8.8, 8.8] | The package ungit before 1.5.20 are vulnerable to Remote Code Execution (RCE) via argument injection. The issue occurs when calling the /api/fetch endpoint. User controlled values (remote and ref) are passed to the git fetch command. By injecting some git options it was possible to get arbitrary command execution.  |
| Git | 2.45.2 | CVE-2022-0514  | MEDIUM            | 6.5        | Business Logic Errors in GitHub repository crater-invoice/crater prior to 6.0.5.   |
| Git | 2.45.2 | CVE-2022-0515  | MEDIUM            | 4.3        | Cross-Site Request Forgery (CSRF) in GitHub repository crater-invoice/crater prior to 6.0.4.   |
| Git | 2.45.2 | CVE-2022-1034  | HIGH              | 7.2        | There is a Unrestricted Upload of File vulnerability in ShowDoc v2.10.3 in GitHub repository star7th/showdoc prior to 2.10.4.  |
| Git | 2.45.2 | CVE-2022-1036  | HIGH              | 7.5        | Able to create an account with long password leads to memory corruption / Integer Overflow in GitHub repository microweber/microweber prior to 1.2.12.   |
| Git | 2.45.2 | CVE-2022-21718 | ['LOW', 'MEDIUM'] | [3.4, 5.0] | Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. A vulnerability in versions prior to `17.0.0-alpha.6`, `16.0.6`, `15.3.5`, `14.2.4`, and `13.6.6` allows renderers to obtain access to a bluetooth device via the web bluetooth API if the app has not configured a custom `select-bluetooth-device` event handler. This has been patched and Electron versions `17.0.0-alpha.6`, `16.0.6`, `15.3.5`, `14.2.4`, and `13.6.6` contain the fix. Code from the GitHub Security Advisory can be added to the app to work around the issue. |
| Git | 2.45.2 | CVE-2022-24764 | ['HIGH', 'HIGH']  | [7.5, 7.5] | PJSIP is a free and open source multimedia communication library written in C. Versions 2.12 and prior contain a stack buffer overflow vulnerability that affects PJSUA2 users or users that call the API `pjmedia_sdp_print()`, `pjmedia_sdp_media_print()`. Applications that do not use PJSUA2 and do not directly call `pjmedia_sdp_print()` or `pjmedia_sdp_media_print()` should not be affected. A patch is available on the `master` branch of the `pjsip/pjproject` GitHub repository. There are currently no known workarounds.  |
| Git | 2.45.2 | CVE-2022-1031  | HIGH              | 7.8        | Use After Free in op_is_set_bp in GitHub repository radareorg/radare2 prior to 5.6.6.  |
| Git | 2.45.2 | CVE-2022-1033  | HIGH              | 7.8        | Unrestricted Upload of File with Dangerous Type in GitHub repository crater-invoice/crater prior to 6.0.6.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-24730 | ['HIGH', 'MEDIUM']   | [7.7, 6.5] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 1.3.0 but before versions 2.1.11, 2.2.6, and 2.3.0 is vulnerable to a path traversal bug, compounded by an improper access control bug, allowing a malicious user with read-only repository access to leak sensitive files from Argo CD's repo-server. A malicious Argo CD user who has been granted `get` access for a repository containing a Helm chart can craft an API request to the `/api/v1/repositories/{repo_url}/appdetails` endpoint to leak the contents of out-of-bounds files from the repo-server. The malicious payload would reference an out-of-bounds file, and the contents of that file would be returned as part of the response. Contents from a non-YAML file may be returned as part of an error message. The attacker would have to know or guess the location of the target file. Sensitive files which could be leaked include files from other Applications' source repositories or any secrets... |
| Git | 2.45.2 | CVE-2022-24731 | ['MEDIUM', 'MEDIUM'] | [6.8, 4.9] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 1.5.0 but before versions 2.1.11, 2.2.6, and 2.3.0 is vulnerable to a path traversal vulnerability, allowing a malicious user with read/write access to leak sensitive files from Argo CD's repo-server. A malicious Argo CD user who has been granted `create` or `update` access to Applications can leak the contents of any text file on the repo-server. By crafting a malicious Helm chart and using it in an Application, the attacker can retrieve the sensitive file's contents either as part of the generated manifests or in an error message. The attacker would have to know or guess the location of the target file. Sensitive files which could be leaked include files from another Application's source repositories or any secrets which have been mounted as files on the repo-server. This vulnerability is patched in Argo CD versions 2.1.11, 2.2.6, and 2.3.0. The problem can be mitigated by avoid... |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-24768 | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All unpatched versions of Argo CD starting with 1.0.0 are vulnerable to an improper access control bug, allowing a malicious user to potentially escalate their privileges to admin-level. Versions starting with 0.8.0 and 0.5.0 contain limited versions of this issue. To perform exploits, an authorized Argo CD user must have push access to an Application's source git or Helm repository or `sync` and `override` access to an Application. Once a user has that access, different exploitation levels are possible depending on their other RBAC privileges. A patch for this vulnerability has been released in Argo CD versions 2.3.2, 2.2.8, and 2.1.14. Some mitigation measures are available but do not serve as a substitute for upgrading. To avoid privilege escalation, limit who has push access to Application source repositories or `sync` + `override` access to Applications; and limit which repositories are available in proje... |
| Git | 2.45.2 | CVE-2022-0315  | HIGH                 | 7.5        | Insecure Temporary File in GitHub repository horovod/horovod prior to 0.24.0.  |
| Git | 2.45.2 | CVE-2022-1061  | HIGH                 | 7.5        | Heap Buffer Overflow in parseDragons in GitHub repository radareorg/radare2 prior to 5.6.8.  |
| Git | 2.45.2 | CVE-2022-0145  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository forkcms/forkcms prior to 5.11.1.  |
| Git | 2.45.2 | CVE-2022-1052  | MEDIUM               | 5.5        | Heap Buffer Overflow in iterate_chained_fixups in GitHub repository radareorg/radare2 prior to 5.6.6.  |
| Git | 2.45.2 | CVE-2022-0955  | MEDIUM               | 4.8        | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/data-hub prior to 1.2.4.  |
| Git | 2.45.2 | CVE-2022-1058  | MEDIUM               | 6.1        | Open Redirect on login in GitHub repository go-gitea/gitea prior to 1.16.5.  |
| Git | 2.45.2 | CVE-2022-0153  | HIGH                 | 7.5        | SQL Injection in GitHub repository forkcms/forkcms prior to 5.11.1.  |
| Git | 2.45.2 | CVE-2022-24782 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Discourse is an open source discussion platform. Versions 2.8.2 and prior in the `stable` branch, 2.9.0.beta3 and prior in the `beta` branch, and 2.9.0.beta3 and prior in the `tests-passed` branch are vulnerable to a data leak. Users can request an export of their own activity. Sometimes, due to category settings, they may have category membership for a secure category. The name of this secure category is shown to the user in the export. The same thing occurs when the user's post has been moved to a secure category. A patch for this issue is available in the `main` branch of Discourse's GitHub repository and is anticipated to be part of future releases.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1064  | HIGH                 | 8.8        | SQL injection through marking blog comments on bulk as spam in GitHub repository forkcms/forkcms prior to 5.11.1.  |
| Git | 2.45.2 | CVE-2022-24784 | ['LOW', 'LOW']       | [3.7, 3.7] | Statamic is a Laravel and Git powered CMS. Before versions 3.2.39 and 3.3.2, it is possible to confirm a single character of a user's password hash using a specially crafted regular expression filter in the users endpoint of the REST API. Multiple such requests can eventually uncover the entire hash. The hash is not present in the response, however the presence or absence of a result confirms if the character is in the right position. The API has throttling enabled by default, making this a time intensive task. Both the REST API and the users endpoint need to be enabled, as they are disabled by default. The issue has been fixed in versions 3.2.39 and above, and 3.3.2 and above. |
| Git | 2.45.2 | CVE-2022-1071  | HIGH                 | 8.2        | User after free in mrb_vm_exec in GitHub repository mruby/mruby prior to 3.2.  |
| Git | 2.45.2 | CVE-2022-1106  | CRITICAL             | 9.1        | use after free in mrb_vm_exec in GitHub repository mruby/mruby prior to 3.2.   |
| Git | 2.45.2 | CVE-2021-39876 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | In all versions of GitLab CE/EE since version 11.3, the endpoint for auto-completing Assignee discloses the members of private groups.   |
| Git | 2.45.2 | CVE-2021-4191  | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab CE/EE affecting versions 13.0 to 14.6.5, 14.7 to 14.7.4, and 14.8 to 14.8.2. Private GitLab instances with restricted sign-ups may be vulnerable to user enumeration to unauthenticated users through the GraphQL API.  |
| Git | 2.45.2 | CVE-2022-0123  | ['MEDIUM', 'MEDIUM'] | [5.9, 6.8] | An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab does not validate SSL certificates for some of external CI services which makes it possible to perform MitM attacks on connections to these external services.  |
| Git | 2.45.2 | CVE-2022-0136  | ['MEDIUM', 'HIGH']   | [5.4, 8.1] | A vulnerability was discovered in GitLab versions 10.5 to 14.5.4, 14.6 to 14.6.4, and 14.7 to 14.7.1. GitLab was vulnerable to a blind SSRF attack through the Project Import feature.   |
| Git | 2.45.2 | CVE-2022-0249  | ['LOW', 'CRITICAL']  | [3.1, 9.1] | A vulnerability was discovered in GitLab starting with version 12. GitLab was vulnerable to a blind SSRF attack since requests to shared address space were not blocked.   |

|     |        |               |                          |             |   |
|-----|--------|---------------|--------------------------|-------------|---|
| Git | 2.45.2 | CVE-2022-0283 | ['MEDIUM', 'MEDIUM']     | [4.7, 6.1]  | An issue has been discovered affecting GitLab versions prior to 13.5. An open redirect vulnerability was fixed in GitLab integration with Jira that a could cause the web application to redirect the request to the attacker specified URL.  |
| Git | 2.45.2 | CVE-2022-0344 | ['LOW', 'MEDIUM']        | [3.1, 4.3]  | An issue has been discovered in GitLab affecting all versions starting from 10.0 before 14.5.4, all versions starting from 10.1 before 14.6.4, all versions starting from 10.2 before 14.7.1. Private project paths can be disclosed to unauthorized users via system notes when an Issue is closed via a Merge Request and later moved to a public project |
| Git | 2.45.2 | CVE-2022-0371 | ['MEDIUM', 'MEDIUM']     | [4.3, 4.3]  | An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.4 before 14.5.4, all versions starting from 14.6 before 14.6.4, all versions starting from 14.7 before 14.7.1. GitLab search may allow authenticated users to search other users by their respective private emails even if a user set their email to private.         |
| Git | 2.45.2 | CVE-2022-0427 | ['HIGH', 'HIGH']         | [7.7, 8.8]  | Missing sanitization of HTML attributes in Jupyter notebooks in all versions of GitLab CE/EE since version 14.5 allows an attacker to perform arbitrary HTTP POST requests on a user's behalf leading to potential account takeover   |
| Git | 2.45.2 | CVE-2022-0488 | ['LOW', 'MEDIUM']        | [3.5, 4.3]  | An issue has been discovered in GitLab CE/EE affecting all versions starting with version 8.10. It was possible to trigger a timeout on a page with markdown by using a specific amount of block-quotes.  |
| Git | 2.45.2 | CVE-2022-0549 | ['MEDIUM', 'MEDIUM']     | [6.5, 6.5]  | An issue has been discovered in GitLab CE/EE affecting all versions before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Under certain conditions, GitLab REST API may allow unprivileged users to add other users to groups even if that is not possible to do through the Web UI.                 |
| Git | 2.45.2 | CVE-2022-0735 | ['CRITICAL', 'CRITICAL'] | [10.0, 9.8] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.10 before 14.6.5, all versions starting from 14.7 before 14.7.4, all versions starting from 14.8 before 14.8.2. An unauthorised user was able to steal runner registration tokens through an information disclosure vulnerability using quick actions commands.        |

|     |        |               |                    |            |   |
|-----|--------|---------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-0738 | ['MEDIUM', 'HIGH'] | [4.2, 7.5] | An issue has been discovered in GitLab affecting all versions starting from 14.6 before 14.6.5, all versions starting from 14.7 before 14.7.4, all versions starting from 14.8 before 14.8.2. GitLab was leaking user passwords when adding mirrors with SSH credentials under specific conditions. |
| Git | 2.45.2 | CVE-2022-0751 | ['MEDIUM', 'HIGH'] | [6.5, 8.8] | Inaccurate display of Snippet files containing special characters in all versions of GitLab CE/EE allows an attacker to create Snippets with misleading content which could trick unsuspecting users into executing arbitrary commands  |
| Git | 2.45.2 | CVE-2022-1032 | HIGH               | 7.2        | Insecure deserialization of not validated module file in GitHub repository crater-invoice/crater prior to 6.0.6.  |
| Git | 2.45.2 | CVE-2022-1163 | MEDIUM             | 4.8        | Cross-site Scripting (XSS) - Stored in GitHub repository mineweb/minewebcms prior to next.  |
| Git | 2.45.2 | CVE-2022-1172 | MEDIUM             | 5.0        | Null Pointer Dereference Caused Segmentation Fault in GitHub repository gpac/gpac prior to 2.1.0-DEV.   |
| Git | 2.45.2 | CVE-2022-1177 | MEDIUM             | 4.3        | Accounting User Can Download Patient Reports in openemr in GitHub repository openemr/openemr prior to 6.1.0.  |
| Git | 2.45.2 | CVE-2022-1154 | HIGH               | 7.8        | Use after free in utf_ptr2char in GitHub repository vim/vim prior to 8.2.4646.  |
| Git | 2.45.2 | CVE-2022-1178 | MEDIUM             | 5.4        | Stored Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.4.  |
| Git | 2.45.2 | CVE-2022-1179 | MEDIUM             | 5.4        | Non-Privilege User Can Created New Rule and Lead to Stored Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.4.  |
| Git | 2.45.2 | CVE-2022-1180 | LOW                | 3.5        | Reflected Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.4.   |
| Git | 2.45.2 | CVE-2022-1181 | MEDIUM             | 5.4        | Stored Cross Site Scripting in GitHub repository openemr/openemr prior to 6.0.0.2.  |
| Git | 2.45.2 | CVE-2022-1155 | HIGH               | 7.4        | Old sessions are not blocked by the login enable function. in GitHub repository snipe/snipe-it prior to 5.3.10.   |
| Git | 2.45.2 | CVE-2022-1160 | HIGH               | 7.8        | heap buffer overflow in get_one_sourceline in GitHub repository vim/vim prior to 8.2.4647.  |
| Git | 2.45.2 | CVE-2022-1191 | HIGH               | 8.1        | SSRF on index.php/cobrowse/proxycss/ in GitHub repository livehelperchat/livehelperchat prior to 3.96.  |
| Git | 2.45.2 | CVE-2022-1176 | HIGH               | 7.5        | Loose comparison causes IDOR on multiple endpoints in GitHub repository livehelperchat/livehelperchat prior to 3.96.  |
| Git | 2.45.2 | CVE-2022-0350 | MEDIUM             | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository vanessa219/vditor prior to 3.8.13.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-21235 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package github.com/masterminds/vcs before 1.13.3 are vulnerable to Command Injection via argument injection. When hg is executed, argument strings are passed to hg in a way that additional flags can be set. The additional flags can be used to perform a command injection.  |
| Git | 2.45.2 | CVE-2022-24440 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package cocoapods-downloader before 1.6.0, from 1.6.2 and before 1.6.3 are vulnerable to Command Injection via git argument injection. When calling the Pod::Downloader.preprocess_options function and using git, both the git and branch parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection. |
| Git | 2.45.2 | CVE-2022-1207  | MEDIUM               | 6.6        | Out-of-bounds read in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability allows attackers to read sensitive information from outside the allocated buffer boundary.  |
| Git | 2.45.2 | CVE-2022-24066 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package simple-git before 3.5.0 are vulnerable to Command Injection due to an incomplete fix of [CVE-2022-24433](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2421199) which only patches against the git fetch attack vector. A similar use of the --upload-pack feature of git is also supported for git clone, which the prior fix didn't cover.   |
| Git | 2.45.2 | CVE-2021-39908 | ['MEDIUM', 'HIGH']   | [6.5, 7.5] | In all versions of GitLab CE/EE starting from 0.8.0 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 certain Unicode characters can be abused to commit malicious code into projects without being noticed in merge request or source code viewer UI.   |
| Git | 2.45.2 | CVE-2022-0373  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper access control in GitLab CE/EE versions 12.4 to 14.5.4, 14.5 to 14.6.4, and 12.6 to 14.7.1 allows project non-members to retrieve the service desk email address  |
| Git | 2.45.2 | CVE-2022-0390  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper access control in Gitlab CE/EE versions 12.7 to 14.5.4, 14.6 to 14.6.4, and 14.7 to 14.7.1 allowed for project non-members to retrieve issue details when it was linked to an item from the vulnerability dashboard.  |
| Git | 2.45.2 | CVE-2022-0425  | ['MEDIUM', 'HIGH']   | [5.4, 7.6] | A DNS rebinding vulnerability in the Irker IRC Gateway integration in all versions of GitLab CE/EE since version 7.9 allows an attacker to trigger Server Side Request Forgery (SSRF) attacks.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-0489  | ['LOW', 'MEDIUM']    | [3.5, 5.7] | An issue has been discovered in GitLab CE/EE affecting all versions starting with 8.15 . It was possible to trigger a DOS by using the math feature with a specific formula in issue comments.   |
| Git | 2.45.2 | CVE-2022-0741  | ['MEDIUM', 'HIGH']   | [5.8, 7.5] | Improper input validation in all versions of GitLab CE/EE using sendmail to send emails allowed an attacker to steal environment variables via specially crafted email addresses.  |
| Git | 2.45.2 | CVE-2022-1201  | MEDIUM               | 6.5        | NULL Pointer Dereference in mrb_vm_exec with super in GitHub repository mruby/mruby prior to 3.2. This vulnerability is capable of making the mruby interpreter crash, thus affecting the availability of the system.  |
| Git | 2.45.2 | CVE-2022-0088  | HIGH                 | 7.4        | Cross-Site Request Forgery (CSRF) in GitHub repository yourls/yourls prior to 1.8.3.   |
| Git | 2.45.2 | CVE-2022-0405  | MEDIUM               | 4.3        | Improper Access Control in GitHub repository janeczku/calibre-web prior to 0.6.16.   |
| Git | 2.45.2 | CVE-2022-0406  | MEDIUM               | 4.3        | Improper Authorization in GitHub repository janeczku/calibre-web prior to 0.6.16.  |
| Git | 2.45.2 | CVE-2022-0939  | CRITICAL             | 9.9        | Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18.  |
| Git | 2.45.2 | CVE-2022-1222  | MEDIUM               | 5.5        | Inf loop in GitHub repository gpac/gpac prior to 2.1.0-DEV.  |
| Git | 2.45.2 | CVE-2022-1223  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Incorrect Authorization in GitHub repository phpipam/phpipam prior to 1.4.6.   |
| Git | 2.45.2 | CVE-2022-1224  | MEDIUM               | 6.5        | Improper Authorization in GitHub repository phpipam/phpipam prior to 1.4.6.  |
| Git | 2.45.2 | CVE-2022-1225  | MEDIUM               | 6.5        | Incorrect Privilege Assignment in GitHub repository phpipam/phpipam prior to 1.4.6.  |
| Git | 2.45.2 | CVE-2022-0990  | CRITICAL             | 9.1        | Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.18.  |
| Git | 2.45.2 | CVE-2022-24813 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. Without the patch for this issue, anonymous comments can be made using Special:RequestWikiQueue when sent directly via POST. A patch for this issue is available in the `master` branch of CreateWiki's GitHub repository.                 |
| Git | 2.45.2 | CVE-2022-0740  | ['LOW', 'MEDIUM']    | [3.1, 4.3] | Incorrect authorization in the Asana integration's branch restriction feature in all versions of GitLab CE/EE starting from version 7.8.0 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 makes it possible to close Asana tasks from unrestricted branches. |

|     |        |               |                          |            |  |
|-----|--------|---------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1099 | ['MEDIUM', 'MEDIUM']     | [4.3, 4.3] | Adding a very large number of tags to a runner in GitLab CE/EE affecting all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an attacker to impact the performance of GitLab   |
| Git | 2.45.2 | CVE-2022-1100 | ['MEDIUM', 'MEDIUM']     | [4.3, 4.3] | A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 13.1 prior to 14.7.7, 14.8.0 prior to 14.8.5, and 14.9.0 prior to 14.9.2. The api to update an asset as a link from a release had a regex check which caused exponential number of backtracks for certain user supplied values resulting in high CPU usage. |
| Git | 2.45.2 | CVE-2022-1105 | ['MEDIUM', 'MEDIUM']     | [4.3, 4.3] | An improper access control vulnerability in GitLab CE/EE affecting all versions from 13.11 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an unauthorized user to access pipeline analytics even when public pipelines are disabled  |
| Git | 2.45.2 | CVE-2022-1111 | ['LOW', 'LOW']           | [2.4, 2.7] | A business logic error in Project Import in GitLab CE/EE versions 14.9 prior to 14.9.2, 14.8 prior to 14.8.5, and 14.0 prior to 14.7.7 under certain conditions caused imported projects to show an incorrect user in the 'Access Granted' column in the project membership pages  |
| Git | 2.45.2 | CVE-2022-1120 | ['MEDIUM', 'MEDIUM']     | [4.8, 6.5] | Missing filtering in an error message in GitLab CE/EE affecting all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 exposed sensitive information when an include directive fails in the CI/CD configuration.   |
| Git | 2.45.2 | CVE-2022-1121 | ['MEDIUM', 'MEDIUM']     | [5.3, 5.3] | A lack of appropriate timeouts in GitLab Pages included in GitLab CE/EE all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows an attacker to cause unlimited resource consumption.   |
| Git | 2.45.2 | CVE-2022-1148 | ['MEDIUM', 'MEDIUM']     | [5.3, 6.5] | Improper authorization in GitLab Pages included with GitLab CE/EE affecting all versions from 11.5 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to steal a user's access token on an attacker-controlled private GitLab Pages website and reuse that token on the victim's other private websites             |
| Git | 2.45.2 | CVE-2022-1162 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.8] | A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1174  | ['MEDIUM', 'HIGH']   | [4.3, 7.5] | A potential DoS vulnerability was discovered in Gitlab CE/EE versions 13.7 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to trigger high CPU usage via a special crafted input added in Issues, Merge requests, Milestones, Snippets, Wiki pages, etc.   |
| Git | 2.45.2 | CVE-2022-1175  | ['HIGH', 'MEDIUM']   | [8.7, 6.1] | Improper neutralization of user input in GitLab CE/EE versions 14.4 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to exploit XSS by injecting HTML in notes.   |
| Git | 2.45.2 | CVE-2022-1185  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | A denial of service vulnerability when rendering RDoc files in GitLab CE/EE versions 10 to 14.7.7, 14.8.0 to 14.8.5, and 14.9.0 to 14.9.2 allows an attacker to crash the GitLab web application with a maliciously crafted RDoc file  |
| Git | 2.45.2 | CVE-2022-1188  | ['LOW', 'MEDIUM']    | [3.7, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 where a blind SSRF attack through the repository mirroring feature was possible.  |
| Git | 2.45.2 | CVE-2022-1189  | ['LOW', 'MEDIUM']    | [3.1, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.2 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 that allowed for an unauthorised user to read the the approval rules of a private project.  |
| Git | 2.45.2 | CVE-2022-1190  | ['HIGH', 'MEDIUM']   | [8.7, 5.4] | Improper handling of user input in GitLab CE/EE versions 8.3 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to exploit a stored XSS by abusing multi-word milestone references in issue descriptions, comments, etc.  |
| Git | 2.45.2 | CVE-2022-1233  | MEDIUM               | 6.1        | URL Confusion When Scheme Not Supplied in GitHub repository medialize/uri.js prior to 1.19.11.   |
| Git | 2.45.2 | CVE-2022-23732 | HIGH                 | 8.8        | A path traversal vulnerability was identified in GitHub Enterprise Server management console that allowed the bypass of CSRF protections. This could potentially lead to privilege escalation. To exploit this vulnerability, an attacker would need to target a user that was actively logged into the management console. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.5 and was fixed in versions 3.1.19, 3.2.11, 3.3.6, 3.4.1. This vulnerability was reported via the GitHub Bug Bounty program. |

|     |        |               |          |     |   |
|-----|--------|---------------|----------|-----|---|
| Git | 2.45.2 | CVE-2022-1212 | CRITICAL | 9.8 | Use-After-Free in str_escape in mruby/mruby in GitHub repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited.  |
| Git | 2.45.2 | CVE-2022-1213 | HIGH     | 8.1 | SSRF filter bypass port 80, 433 in GitHub repository livehelperchat/livehelperchat prior to 3.67v. An attacker could make the application perform arbitrary requests, bypass CVE-2022-1191  |
| Git | 2.45.2 | CVE-2022-1235 | HIGH     | 8.2 | Weak secrethash can be brute-forced in GitHub repository livehelperchat/livehelperchat prior to 3.96.   |
| Git | 2.45.2 | CVE-2022-1236 | MEDIUM   | 6.5 | Weak Password Requirements in GitHub repository weseek/growi prior to v5.0.0.   |
| Git | 2.45.2 | CVE-2022-1243 | MEDIUM   | 6.1 | CRHTLF can lead to invalid protocol extraction potentially leading to XSS in GitHub repository medialize/uri.js prior to 1.19.11.   |
| Git | 2.45.2 | CVE-2022-0602 | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - DOM in GitHub repository tastyigniter/tastyigniter prior to 3.3.0.   |
| Git | 2.45.2 | CVE-2022-1244 | MEDIUM   | 5.5 | heap-buffer-overflow in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of inducing denial of service.  |
| Git | 2.45.2 | CVE-2022-1234 | MEDIUM   | 6.1 | XSS in livehelperchat in GitHub repository livehelperchat/livehelperchat prior to 3.97. This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.   |
| Git | 2.45.2 | CVE-2022-1237 | HIGH     | 7.8 | Improper Validation of Array Index in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is heap overflow and may be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/122.html).   |
| Git | 2.45.2 | CVE-2022-1238 | HIGH     | 7.8 | Out-of-bounds Write in libr/bin/format/ne/ne.c in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is heap overflow and may be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/122.html).   |
| Git | 2.45.2 | CVE-2022-1240 | HIGH     | 7.8 | Heap buffer overflow in libr/bin/format/mach0/mach0.c in GitHub repository radareorg/radare2 prior to 5.8.6. If address sanitizer is disabled during the compiling, the program should executes into the `r_strncpy` function. Therefore I think it is very likely to be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/122.html). |

|     |        |                |                          |            |   |
|-----|--------|----------------|--------------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1253  | CRITICAL                 | 9.8        | Heap-based Buffer Overflow in GitHub repository strukturag/libde265 prior to and including 1.0.8. The fix is established in commit 8e89fe0e175d2870c39486fdd09250b230ec10b8 but does not yet belong to an official release.   |
| Git | 2.45.2 | CVE-2022-24786 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | PJSIP is a free and open source multimedia communication library written in C. PJSIP versions 2.12 and prior do not parse incoming RTCP feedback RPSI (Reference Picture Selection Indication) packet, but any app that directly uses pjmedia_rtcp_fb_parse_rpsi() will be affected. A patch is available in the `master` branch of the `pjsip/pjproject` GitHub repository. There are currently no known workarounds.  |
| Git | 2.45.2 | CVE-2022-24793 | ['HIGH', 'HIGH']         | [7.5, 7.5] | PJSIP is a free and open source multimedia communication library written in C. A buffer overflow vulnerability in versions 2.12 and prior affects applications that use PJSIP DNS resolution. It doesn't affect PJSIP users who utilize an external resolver. This vulnerability is related to CVE-2023-27585. The difference is that this issue is in parsing the query record `parse_rr()`, while the issue in CVE-2023-27585 is in `parse_query()`. A patch is available in the `master` branch of the `pjsip/pjproject` GitHub repository. A workaround is to disable DNS resolution in PJSIP config (by setting `nameserver_count` to zero) or use an external resolver instead. |
| Git | 2.45.2 | CVE-2022-0935  | HIGH                     | 8.8        | Host Header injection in password Reset in GitHub repository livehelperchat/livehelperchat prior to 3.97.   |
| Git | 2.45.2 | CVE-2022-1219  | HIGH                     | 7.5        | SQL injection in RecyclebinController.php in GitHub repository pimcore/pimcore prior to 10.3.5. This vulnerability is capable of steal the data   |
| Git | 2.45.2 | CVE-2022-1283  | MEDIUM                   | 5.5        | NULL Pointer Dereference in r_bin_ne_get_entrypoints function in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability allows attackers to cause a denial of service (application crash).  |
| Git | 2.45.2 | CVE-2022-1284  | MEDIUM                   | 5.5        | heap-use-after-free in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of inducing denial of service.   |
| Git | 2.45.2 | CVE-2022-1276  | CRITICAL                 | 9.8        | Out-of-bounds Read in mrb_get_args in GitHub repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited.   |
| Git | 2.45.2 | CVE-2022-1286  | CRITICAL                 | 9.8        | heap-buffer-overflow in mrb_vm_exec in mruby/mruby in GitHub repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited.   |

|     |        |               |                      |            |  |
|-----|--------|---------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1290 | MEDIUM               | 5.4        | Stored XSS in "Name", "Group Name" & "Title" in GitHub repository polonel/trudesk prior to v1.2.0. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.  |
| Git | 2.45.2 | CVE-2022-1291 | MEDIUM               | 5.4        | XSS vulnerability with default `onCellHtmlData` function in GitHub repository hhurz/tableexport.jquery.plugin prior to 1.25.0. Transmitting cookies to third-party servers. Sending data from secure sessions to third-party servers   |
| Git | 2.45.2 | CVE-2022-0936 | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository autolab/autolab prior to 2.8.0.   |
| Git | 2.45.2 | CVE-2022-1045 | MEDIUM               | 5.4        | Stored XSS viva .svg file upload in GitHub repository polonel/trudesk prior to v1.2.0.   |
| Git | 2.45.2 | CVE-2022-1252 | ['HIGH', 'CRITICAL'] | [8.2, 9.1] | Use of a Broken or Risky Cryptographic Algorithm in GitHub repository gnuboard/gnuboard5 prior to and including 5.5.5. A vulnerability in gnuboard v5.5.5 and below uses weak encryption algorithms leading to sensitive information exposure. This allows an attacker to derive the email address of any user, including when the 'Let others see my information.' box is ticked off. Or to send emails to any email address, with full control of its contents |
| Git | 2.45.2 | CVE-2022-1295 | CRITICAL             | 9.8        | Prototype Pollution in GitHub repository alvarotrigo/fullpage.js prior to 4.0.2.   |
| Git | 2.45.2 | CVE-2022-1296 | CRITICAL             | 9.1        | Out-of-bounds read in `r_bin_ne_get_relocs` function in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability may allow attackers to read sensitive information or cause a crash.   |
| Git | 2.45.2 | CVE-2022-1297 | CRITICAL             | 9.1        | Out-of-bounds Read in r_bin_ne_get_entrypoints function in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability may allow attackers to read sensitive information or cause a crash.  |
| Git | 2.45.2 | CVE-2022-1157 | ['LOW', 'LOW']       | [2.6, 2.4] | Missing sanitization of logged exception messages in all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 of GitLab CE/EE causes potential sensitive values in invalid URLs to be logged   |
| Git | 2.45.2 | CVE-2022-1193 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper access control in GitLab CE/EE versions 10.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allows a malicious actor to obtain details of the latest commit in a private project via Merge Requests under certain circumstances  |
| Git | 2.45.2 | CVE-2022-1316 | ['HIGH', 'HIGH']     | [8.8, 7.8] | Incorrect Permission Assignment for Critical Resource in GitHub repository zerotier/zerotierone prior to 1.8.8. Local Privilege Escalation   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-24765 | ['MEDIUM', 'HIGH'] | [6.0, 7.8] | Git for Windows is a fork of Git containing Windows-specific patches. This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk. Those untrusted parties could create the folder `C:\.git`, which would be picked up by Git operations run supposedly outside a repository while searching for a Git directory. Git would then respect any config in said Git directory. Git Bash users who set `GIT_PS1_SHOWDIRTYSTATE` are vulnerable as well. Users who installed posh-git are vulnerable simply by starting a PowerShell. Users of IDEs such as Visual Studio are vulnerable: simply creating a new project would already read and respect the config specified in `C:\.git\config`. Users of the Microsoft fork of Git are vulnerable simply by starting a Git Bash. The problem has been patched in Git for Windows v2.35.2. Users unable to upgrade may create the folder `.git` on all drives where Git commands are run, and remove read/write access ... |
| Git | 2.45.2 | CVE-2022-24767 | ['HIGH', 'HIGH']   | [7.8, 7.8] | GitHub: Git for Windows' uninstaller vulnerable to DLL hijacking when run under the SYSTEM user account.  |
| Git | 2.45.2 | CVE-2022-29040 | MEDIUM             | 5.4        | Jenkins Git Parameter Plugin 0.9.15 and earlier does not escape the name and description of Git parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.  |
| Git | 2.45.2 | CVE-2022-0436  | MEDIUM             | 5.5        | Path Traversal in GitHub repository gruntjs/grunt prior to 1.5.2.   |
| Git | 2.45.2 | CVE-2022-1330  | MEDIUM             | 5.4        | stored xss due to unsanitized anchor url in GitHub repository alvarotrigo/fullpage.js prior to 4.0.4. stored xss .  |
| Git | 2.45.2 | CVE-2022-1339  | HIGH               | 7.5        | SQL injection in ElementController.php in GitHub repository pimcore/pimcore prior to 10.3.5. This vulnerability is capable of steal the data  |
| Git | 2.45.2 | CVE-2022-1344  | CRITICAL           | 9.0        | Stored XSS due to no sanitization in the filename in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.   |
| Git | 2.45.2 | CVE-2022-1346  | CRITICAL           | 9.0        | Multiple Stored XSS in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.   |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1345  | CRITICAL         | 9.0        | Stored XSS via .svg file upload in GitHub repository causefx/organizr prior to 2.1.1810. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.   |
| Git | 2.45.2 | CVE-2022-1347  | HIGH             | 8.4        | Stored XSS in the "Username" & "Email" input fields leads to account takeover of Admin & Co-admin users in GitHub repository causefx/organizr prior to 2.1.1810. Account takeover and privilege escalation  |
| Git | 2.45.2 | CVE-2022-24828 | ['HIGH', 'HIGH'] | [8.3, 8.8] | Composer is a dependency manager for the PHP programming language. Integrators using Composer code to call `VcsDriver::getFileContent` can have a code injection vulnerability if the user can control the `\$file` or `\$identifier` argument. This leads to a vulnerability on packagist.org for example where the composer.json's `readme` field can be used as a vector for injecting parameters into hg/Mercurial via the `\$file` argument, or git via the `\$identifier` argument if you allow arbitrary data there (Packagist does not, but maybe other integrators do). Composer itself should not be affected by the vulnerability as it does not call `getFileContent` with arbitrary data into `\$file`/`\$identifier`. To the best of our knowledge this was not abused, and the vulnerability has been patched on packagist.org and Private Packagist within a day of the vulnerability report. |
| Git | 2.45.2 | CVE-2022-1351  | MEDIUM           | 5.4        | Stored XSS in Tooltip in GitHub repository pimcore/pimcore prior to 10.4.   |
| Git | 2.45.2 | CVE-2021-43286 | HIGH             | 8.8        | An issue was discovered in ThoughtWorks GoCD before 21.3.0. An attacker with privileges to create a new pipeline on a GoCD server can abuse a command-line injection in the Git URL "Test Connection" feature to execute arbitrary code.  |
| Git | 2.45.2 | CVE-2022-1231  | MEDIUM           | 6.1        | XSS via Embedded SVG in SVG Diagram Format in GitHub repository plantuml/plantuml prior to 1.2022.4. Stored XSS in the context of the diagram embedder. Depending on the actual context, this ranges from stealing secrets to account hijacking or even to code execution for example in desktop applications. Web based applications are the ones most affected. Since the SVG format allows clickable links in diagrams, it is commonly used in plugins for web based projects (like the Confluence plugin, etc. see <a href="https://plantuml.com/de/running">https://plantuml.com/de/running</a> ).   |
| Git | 2.45.2 | CVE-2022-1365  | MEDIUM           | 6.5        | Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository lquixada/cross-fetch prior to 3.1.5.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1380  | MEDIUM               | 5.4        | Stored Cross Site Scripting vulnerability in Item name parameter in GitHub repository snipe/snipe-it prior to v5.4.3. The vulnerability is capable of stolen the user Cookie.  |
| Git | 2.45.2 | CVE-2022-1381  | HIGH                 | 7.8        | global heap buffer overflow in skip_range in GitHub repository vim/vim prior to 8.2.4763. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution  |
| Git | 2.45.2 | CVE-2022-1382  | MEDIUM               | 5.5        | NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of making the radare2 crash, thus affecting the availability of the system.  |
| Git | 2.45.2 | CVE-2022-1383  | MEDIUM               | 6.1        | Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.8. The bug causes the program reads data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.   |
| Git | 2.45.2 | CVE-2022-0645  | MEDIUM               | 6.1        | Open redirect vulnerability via endpoint authorize_and_redirect/?redirect= in GitHub repository posthog/posthog prior to 1.34.1.   |
| Git | 2.45.2 | CVE-2022-25648 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package git before 1.11.0 are vulnerable to Command Injection via git argument injection. When calling the fetch(remote = 'origin', opts = {}) function, the remote parameter is passed to the git fetch subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.  |
| Git | 2.45.2 | CVE-2022-24826 | ['CRITICAL', 'HIGH'] | [9.8, 7.8] | On Windows, if Git LFS operates on a malicious repository with a `..exe` file as well as a file named `git.exe`, and `git.exe` is not found in `PATH`, the `..exe` program will be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. Similarly, if the malicious repository contains files named `..exe` and `cygpath.exe`, and `cygpath.exe` is not found in `PATH`, the `..exe` program will be executed when certain Git LFS commands are run. More generally, if the current working directory contains any file with a base name of `.` and a file extension from `PATHEXT` (except `.bat` and `.cmd`), and also contains another file with the same base name as a program Git LFS intends to execute (such as `git`, `cygpath`, or `uname`) and any file extension from `PATHEXT` (including `.bat` and `.cmd`), then, on Windows, when Git LFS attempts to execute the intended program the `..exe`, `..com`, etc., file will be executed instead, but only if the intended pro... |

|     |        |               |          |     |  |
|-----|--------|---------------|----------|-----|--|
| Git | 2.45.2 | CVE-2022-1420 | MEDIUM   | 5.5 | Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4774.   |
| Git | 2.45.2 | CVE-2022-1022 | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.5.0.   |
| Git | 2.45.2 | CVE-2022-0272 | CRITICAL | 9.8 | Improper Restriction of XML External Entity Reference in GitHub repository detekt/detekt prior to 1.20.0.  |
| Git | 2.45.2 | CVE-2022-1429 | HIGH     | 7.5 | SQL injection in GridHelperService.php in GitHub repository pimcore/pimcore prior to 10.3.6. This vulnerability is capable of steal the data   |
| Git | 2.45.2 | CVE-2022-1437 | HIGH     | 7.1 | Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program reads data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.   |
| Git | 2.45.2 | CVE-2022-1439 | MEDIUM   | 6.1 | Reflected XSS on demo.microweber.org/demo/module/ in GitHub repository microweber/microweber prior to 1.2.15. Execute Arbitrary JavaScript as the attacked user. It's the only payload I found working, you might need to press "tab" but there is probably a payload that runs without user interaction.  |
| Git | 2.45.2 | CVE-2022-1440 | CRITICAL | 9.8 | Command Injection vulnerability in git-interface@2.1.1 in GitHub repository yarkeev/git-interface prior to 2.1.2. If both are provided by user input, then the use of a `--upload-pack` command-line argument feature of git is also supported for `git clone`, which would then allow for any operating system command to be spawned by the attacker. |
| Git | 2.45.2 | CVE-2022-1427 | HIGH     | 7.8 | Out-of-bounds Read in mrb_obj_is_kind_of in in GitHub repository mruby/mruby prior to 3.2. # Impact: Possible arbitrary code execution if being exploited.   |
| Git | 2.45.2 | CVE-2022-1444 | MEDIUM   | 5.5 | heap-use-after-free in GitHub repository radareorg/radare2 prior to 5.7.0. This vulnerability is capable of inducing denial of service.  |
| Git | 2.45.2 | CVE-2022-1445 | MEDIUM   | 5.4 | Stored Cross Site Scripting vulnerability in the checked_out_to parameter in GitHub repository snipe/snipe-it prior to 5.4.3. The vulnerability is capable of stolen the user Cookie.  |

|     |        |                |                  |            |   |
|-----|--------|----------------|------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1451  | HIGH             | 7.1        | Out-of-bounds Read in <code>r_bin_java_constant_value_attr_new</code> function in GitHub repository <code>radareorg/radare2</code> prior to 5.7.0. The bug causes the program reads data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. More details see [CWE-125: Out-of-bounds read](https://cwe.mitre.org/data/definitions/125.html).  |
| Git | 2.45.2 | CVE-2022-1452  | HIGH             | 7.1        | Out-of-bounds Read in <code>r_bin_java_bootstrap_methods_attr_new</code> function in GitHub repository <code>radareorg/radare2</code> prior to 5.7.0. The bug causes the program reads data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. More details see [CWE-125: Out-of-bounds read](https://cwe.mitre.org/data/definitions/125.html).   |
| Git | 2.45.2 | CVE-2022-1457  | MEDIUM           | 5.4        | Store XSS in title parameter executing at <code>EditUserPage</code> & <code>EditProduct</code> page in GitHub repository <code>neorazorx/facturascripts</code> prior to 2022.04. Cross-site scripting attacks can have devastating consequences. Code injected into a vulnerable application can exfiltrate data or install malware on the user's machine. Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.   |
| Git | 2.45.2 | CVE-2022-1458  | MEDIUM           | 5.4        | Stored XSS Leads To Session Hijacking in GitHub repository <code>openemr/openemr</code> prior to 6.1.0.1.   |
| Git | 2.45.2 | CVE-2022-1459  | HIGH             | 8.3        | Non-Privilege User Can View Patient's Disclosures in GitHub repository <code>openemr/openemr</code> prior to 6.1.0.1.   |
| Git | 2.45.2 | CVE-2022-1461  | MEDIUM           | 6.5        | Non Privilege User can Enable or Disable Registered in GitHub repository <code>openemr/openemr</code> prior to 6.1.0.1.   |
| Git | 2.45.2 | CVE-2022-24792 | ['HIGH', 'HIGH'] | [7.5, 7.5] | PJSIP is a free and open source multimedia communication library written in C. A denial-of-service vulnerability affects applications on a 32-bit systems that use PJSIP versions 2.12 and prior to play/read invalid WAV files. The vulnerability occurs when reading WAV file data chunks with length greater than 31-bit integers. The vulnerability does not affect 64-bit apps and should not affect apps that only plays trusted WAV files. A patch is available on the `master` branch of the `pjsip/project` GitHub repository. As a workaround, apps can reject a WAV file received from an unknown source or validate the file first. |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-0477  | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | An issue has been discovered in GitLab affecting all versions starting from 11.9 before 14.5.4, all versions starting from 14.6.0 before 14.6.4, all versions starting from 14.7.0 before 14.7.1. GitLab was not correctly handling bulk requests to delete existing packages from the package registries which could result in a Denial of Service under specific conditions.  |
| Git | 2.45.2 | CVE-2022-25866 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package czproject/git-php before 4.0.3 are vulnerable to Command Injection via git argument injection. When calling the isRemoteUrlReadable(\$url, array \$refs = NULL) function, both the url and refs parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.   |
| Git | 2.45.2 | CVE-2022-1173  | MEDIUM               | 5.4        | stored xss in GitHub repository getgrav/grav prior to 1.7.33.   |
| Git | 2.45.2 | CVE-2022-1504  | MEDIUM               | 6.1        | XSS in /demo/module/?module=HERE in GitHub repository microweber/microweber prior to 1.2.15. Typical impact of XSS attacks.   |
| Git | 2.45.2 | CVE-2022-1507  | MEDIUM               | 5.5        | chafa: NULL Pointer Dereference in function gif_internal_decode_frame at libnsgif.c:599 allows attackers to cause a denial of service (crash) via a crafted input file. in GitHub repository hpjansson/chafa prior to 1.10.2. chafa: NULL Pointer Dereference in function gif_internal_decode_frame at libnsgif.c:599 allows attackers to cause a denial of service (crash) via a crafted input file.                                 |
| Git | 2.45.2 | CVE-2022-1509  | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | Command Injection Vulnerability in GitHub repository hestiacp/hestiacp prior to 1.5.12. An authenticated remote attacker with low privileges can execute arbitrary code under root context.   |
| Git | 2.45.2 | CVE-2022-1511  | MEDIUM               | 6.5        | Missing Authorization in GitHub repository snipe/snipe-it prior to 5.4.4.   |
| Git | 2.45.2 | CVE-2022-1514  | MEDIUM               | 5.4        | Stored XSS via upload plugin functionality in zip format in GitHub repository neorazorx/facturascripts prior to 2022.06. Cross-site scripting attacks can have devastating consequences. Code injected into a vulnerable application can exfiltrate data or install malware on the user's machine. Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account. |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1530  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) in GitHub repository livehelperchat/livehelperchat prior to 3.99v. The attacker can execute malicious JavaScript on the application.   |
| Git | 2.45.2 | CVE-2022-1531  | CRITICAL             | 9.8        | SQL injection vulnerability in ARAX-UI Synonym Lookup functionality in GitHub repository rtxteam/rtx prior to checkpoint_2022-04-20 . This vulnerability is critical as it can lead to remote code execution and thus complete server takeover.   |
| Git | 2.45.2 | CVE-2022-1533  | HIGH                 | 7.8        | Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11. This vulnerability is capable of arbitrary code execution.  |
| Git | 2.45.2 | CVE-2022-1534  | HIGH                 | 7.1        | Buffer Over-read at parse_rawml.c:1416 in GitHub repository bfabiszewski/libmobi prior to 0.11. The bug causes the program reads data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.  |
| Git | 2.45.2 | CVE-2022-24900 | ['CRITICAL', 'HIGH'] | [9.9, 8.6] | Piano LED Visualizer is software that allows LED lights to light up as a person plays a piano connected to a computer. Version 1.3 and prior are vulnerable to a path traversal attack. The <code>`os.path.join`</code> call is unsafe for use with untrusted input. When the <code>`os.path.join`</code> call encounters an absolute path, it ignores all the parameters it has encountered till that point and starts working with the new absolute path. Since the "malicious" parameter represents an absolute path, the result of <code>`os.path.join`</code> ignores the static directory completely. Hence, untrusted input is passed via the <code>`os.path.join`</code> call to <code>`flask.send_file`</code> can lead to path traversal attacks. A patch with a fix is available on the <code>`master`</code> branch of the GitHub repository. This can also be fixed by preventing flow of untrusted data to the vulnerable <code>`send_file`</code> function. In case the application logic necessitates this behaviour, one can either use the <code>`flask.safe_join`</code> to join untrusted paths or replace <code>`flask.send_file`</code> ... |
| Git | 2.45.2 | CVE-2022-1543  | HIGH                 | 8.8        | Improper handling of Length parameter in GitHub repository erudika/scoold prior to 1.49.4. When the text size is large enough the service results in a momentary outage in a production environment. That can lead to memory corruption on the server.  |
| Git | 2.45.2 | CVE-2022-1544  | HIGH                 | 7.8        | Formula Injection/CSV Injection due to Improper Neutralization of Formula Elements in CSV File in GitHub repository luyadev/yii-helpers prior to 1.2.1. Successful exploitation can lead to impacts such as client-sided command injection, code execution, or remote ex-filtration of contained confidential data.   |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2022-24437 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | The package git-pull-or-clone before 2.0.2 are vulnerable to Command Injection due to the use of the --upload-pack feature of git which is also supported for git clone. The source includes the use of the secure child process API spawn(). However, the outpath parameter passed to it may be a command-line argument to the git clone command and result in arbitrary command injection. |
| Git | 2.45.2 | CVE-2022-25850 | ['HIGH', 'HIGH']         | [7.5, 7.5] | The package github.com/hoppscotch/proxyscotch before 1.0.0 are vulnerable to Server-side Request Forgery (SSRF) when interceptor mode is set to proxy. It occurs when an HTTP request is made by a backend server to an untrusted URL submitted by a user. It leads to a leakage of sensitive information from the server.   |
| Git | 2.45.2 | CVE-2022-1554  | HIGH                     | 7.5        | Path Traversal due to `send_file` call in GitHub repository clinical-genomics/scout prior to 4.52.   |
| Git | 2.45.2 | CVE-2021-41959 | HIGH                     | 7.5        | JerryScript Git version 14ff5bf does not sufficiently track and release allocated memory via jerry-core/ecma/operations/ecma-regexp-object.c after RegExp, which causes a memory leak.   |
| Git | 2.45.2 | CVE-2022-27313 | HIGH                     | 7.5        | An arbitrary file deletion vulnerability in Gitea v1.16.3 allows attackers to cause a Denial of Service (DoS) via deleting the configuration file.   |
| Git | 2.45.2 | CVE-2022-1502  | MEDIUM                   | 4.3        | Permissions were not properly verified in the API on projects using version control in Git. This allowed projects to be modified by users with only ProjectView permissions.   |
| Git | 2.45.2 | CVE-2022-1555  | MEDIUM                   | 6.1        | DOM XSS in microweber ver 1.2.15 in GitHub repository microweber/microweber prior to 1.2.16. inject arbitrary js code, deface website, steal cookie...   |
| Git | 2.45.2 | CVE-2022-1571  | MEDIUM                   | 6.1        | Cross-site scripting - Reflected in Create Subaccount in GitHub repository neorazorx/facturascripts prior to 2022.07. This vulnerability can be arbitrarily executed javascript code to steal user's cookie, perform HTTP request, get content of `same origin` page, etc ...  |
| Git | 2.45.2 | CVE-2022-1584  | MEDIUM                   | 6.1        | Reflected XSS in GitHub repository microweber/microweber prior to 1.2.16. Executing JavaScript as the victim   |
| Git | 2.45.2 | CVE-2022-1411  | MEDIUM                   | 6.1        | Unrestricted file upload in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. Attacker can send malicious files to the victims is able to retrieve the stored data from the web application without that data being made safe to render in the browser and steals victim's cookie leads to account takeover.   |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1592  | HIGH               | 8.2        | Server-Side Request Forgery in scout in GitHub repository clinical-genomics/scout prior to v4.42. An attacker could make the application perform arbitrary requests to fishing steal cookie, request to private area, or lead to xss...  |
| Git | 2.45.2 | CVE-2022-1575  | CRITICAL           | 9.6        | Arbitrary Code Execution through Sanitizer Bypass in GitHub repository jgraph/drawio prior to 18.0.0. - Arbitrary (remote) code execution in the desktop app. - Stored XSS in the web app.   |
| Git | 2.45.2 | CVE-2022-1464  | MEDIUM             | 5.4        | Stored xss bug in GitHub repository gogs/gogs prior to 0.12.7. As the repo is public , any user can view the report and when open the attachment then xss is executed. This bug allow executed any javascript code in victim account .   |
| Git | 2.45.2 | CVE-2022-29171 | ['MEDIUM', 'HIGH'] | [6.6, 7.2] | Sourcegraph is a fast and featureful code search and navigation engine. Versions before 3.38.0 are vulnerable to Remote Code Execution in the gitserver service. The Gitolite code host integration with Phabricator allows Sourcegraph site admins to specify a `callsignCommand`, which is used to obtain the Phabricator metadata for a Gitolite repository. An administrator who is able to edit or add a Gitolite code host and has administrative access to Sourcegraph's bundled Grafana instance can change this command arbitrarily and run it remotely. This grants direct access to the infrastructure underlying the Sourcegraph installation. The attack requires: site-admin privileges on the instance of Sourcegraph, Administrative privileges on the bundled Grafana monitoring instance, Knowledge of the gitserver IP address or DNS name (if running in Kubernetes). This can be found through Grafana. The issue is patched in version 3.38.0. You may disable Gitolite code hosts. We still highly encourage... |
| Git | 2.45.2 | CVE-2022-1616  | HIGH               | 7.8        | Use after free in append_command in GitHub repository vim/vim prior to 8.2.4895. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution   |
| Git | 2.45.2 | CVE-2022-1619  | HIGH               | 7.8        | Heap-based Buffer Overflow in function cmdline_erase_chars in GitHub repository vim/vim prior to 8.2.4899. This vulnerabilities are capable of crashing software, modify memory, and possible remote execution   |

|     |        |               |      |     |   |
|-----|--------|---------------|------|-----|---|
| Git | 2.45.2 | CVE-2022-1620 | HIGH | 7.5 | NULL Pointer Dereference in function vim_regex_string at regexp.c:2729 in GitHub repository vim/vim prior to 8.2.4901. NULL Pointer Dereference in function vim_regex_string at regexp.c:2729 allows attackers to cause a denial of service (application crash) via a crafted input.  |
| Git | 2.45.2 | CVE-2022-1631 | HIGH | 8.8 | Users Account Pre-Takeover or Users Account Takeover. in GitHub repository microweber/microweber prior to 1.2.15. Victim Account Take Over. Since, there is no email confirmation, an attacker can easily create an account in the application using the Victim's Email. This allows an attacker to gain pre-authentication to the victim's account. Further, due to the lack of proper validation of email coming from Social Login and failing to check if an account already exists, the victim will not identify if an account is already existing. Hence, the attacker's persistence will remain. An attacker would be able to see all the activities performed by the victim user impacting the confidentiality and attempt to modify/corrupt the data impacting the integrity and availability factor. This attack becomes more interesting when an attacker can register an account from an employee's email address. Assuming the organization uses G-Suite, it is much more impactful to hijack into an employee's... |
| Git | 2.45.2 | CVE-2022-1397 | HIGH | 8.8 | API Privilege Escalation in GitHub repository alexselegidis/easyappointments prior to 1.5.0. Full system takeover.  |
| Git | 2.45.2 | CVE-2022-1537 | HIGH | 7.0 | file.copy operations in GruntJS are vulnerable to a TOCTOU race condition leading to arbitrary file write in GitHub repository gruntjs/grunt prior to 1.5.3. This vulnerability is capable of arbitrary file writes which can lead to local privilege escalation to the GruntJS user if a lower-privileged user has write access to both source and destination directories as the lower-privileged user can create a symlink to the GruntJS user's .bashrc file or replace /etc/shadow file if the GruntJS user is root.   |
| Git | 2.45.2 | CVE-2022-1621 | HIGH | 7.8 | Heap buffer overflow in vim_strncpy find_word in GitHub repository vim/vim prior to 8.2.4919. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution   |
| Git | 2.45.2 | CVE-2022-1629 | HIGH | 7.8 | Buffer Over-read in function find_next_quote in GitHub repository vim/vim prior to 8.2.4925. This vulnerabilities are capable of crashing software, Modify Memory, and possible remote execution  |

|     |        |               |                      |            |   |
|-----|--------|---------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1649 | MEDIUM               | 5.5        | Null pointer dereference in lib/bin/format/mach0/mach0.c in radareorg/radare2 in GitHub repository radareorg/radare2 prior to 5.7.0. It is likely to be exploitable. For more general description of heap buffer overflow, see [CWE](https://cwe.mitre.org/data/definitions/476.html) .   |
| Git | 2.45.2 | CVE-2022-1417 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Improper access control in GitLab CE/EE affecting all versions starting from 8.12 before 14.8.6, all versions starting from 14.9 before 14.9.4, and all versions starting from 14.10 before 14.10.1 allows non-project members to access contents of Project Members-only Wikis via malicious CI jobs   |
| Git | 2.45.2 | CVE-2022-1431 | ['MEDIUM', 'MEDIUM'] | [4.3, 5.3] | An issue has been discovered in GitLab affecting all versions starting from 12.10 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not correctly handling malicious requests to the PyPi API endpoint allowing the attacker to cause uncontrolled resource consumption.                  |
| Git | 2.45.2 | CVE-2022-1124 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An improper authorization issue has been discovered in GitLab CE/EE affecting all versions prior to 14.8.6, all versions from 14.9.0 prior to 14.9.4, and 14.10.0, allowing Guest project members to access trace log of jobs when it is enabled  |
| Git | 2.45.2 | CVE-2022-1352 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Due to an insecure direct object reference vulnerability in Gitlab EE/CE affecting all versions from 11.0 prior to 14.8.6, 14.9 prior to 14.9.4, and 14.10 prior to 14.10.1, an endpoint may reveal the issue title to a user who crafted an API call with the ID of the issue from a public project that restricts access to issue only to project members.      |
| Git | 2.45.2 | CVE-2022-1406 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Improper input validation in GitLab CE/EE affecting all versions from 8.12 prior to 14.8.6, all versions from 14.9.0 prior to 14.9.4, and 14.10.0 allows a Developer to read protected Group or Project CI/CD variables by importing a malicious project  |
| Git | 2.45.2 | CVE-2022-1426 | ['LOW', 'LOW']       | [2.0, 3.7] | An issue has been discovered in GitLab affecting all versions starting from 12.6 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not correctly authenticating a user that had some certain amount of information which allowed an user to authenticate without a personal access token. |

|     |        |               |                      |            |  |
|-----|--------|---------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1428 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab affecting all versions before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was incorrectly verifying throttling limits for authenticated package requests which resulted in limits not being enforced.  |
| Git | 2.45.2 | CVE-2022-1433 | ['LOW', 'MEDIUM']    | [2.6, 6.1] | An issue has been discovered in GitLab affecting all versions starting from 14.4 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. Missing invalidation of Markdown caching causes potential payloads from a previously exploitable XSS vulnerability (CVE-2022-1175) to persist and execute.       |
| Git | 2.45.2 | CVE-2022-1460 | ['MEDIUM', 'MEDIUM'] | [6.1, 4.9] | An issue has been discovered in GitLab affecting all versions starting from 9.2 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not performing correct authorizations on scheduled pipelines allowing a malicious user to run a pipeline in the context of another user.               |
| Git | 2.45.2 | CVE-2022-1510 | ['MEDIUM', 'HIGH']   | [6.5, 7.5] | An issue has been discovered in GitLab affecting all versions starting from 13.9 before 14.8.6, all versions starting from 14.9 before 14.9.4, all versions starting from 14.10 before 14.10.1. GitLab was not correctly handling malicious text in the CI Editor and CI Pipeline details page allowing the attacker to cause uncontrolled resource consumption. |
| Git | 2.45.2 | CVE-2022-1545 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | It was possible to disclose details of confidential notes created via the API in Gitlab CE/EE affecting all versions from 13.2 prior to 14.8.6, 14.9 prior to 14.9.4, and 14.10 prior to 14.10.1 if an unauthorised project member was tagged in the note.   |
| Git | 2.45.2 | CVE-2022-1044 | MEDIUM               | 6.5        | Sensitive Data Exposure Due To Insecure Storage Of Profile Image in GitHub repository polonel/trudesk prior to v1.2.1.   |
| Git | 2.45.2 | CVE-2022-1681 | HIGH                 | 7.2        | Authentication Bypass Using an Alternate Path or Channel in GitHub repository requarks/wiki prior to 2.5.281. User can get root user permissions   |
| Git | 2.45.2 | CVE-2022-1682 | MEDIUM               | 6.1        | Reflected Xss using url based payload in GitHub repository neorazorx/facturascripts prior to 2022.07. Xss can use to steal user's cookies which lead to Account takeover or do any malicious activity in victim's browser  |
| Git | 2.45.2 | CVE-2022-1650 | ['HIGH', 'CRITICAL'] | [8.1, 9.3] | Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository eventsource/eventsource prior to v2.0.2.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-1674  | MEDIUM               | 5.5        | NULL Pointer Dereference in function vim_regex_string at regexp.c:2733 in GitHub repository vim/vim prior to 8.2.4938. NULL Pointer Dereference in function vim_regex_string at regexp.c:2733 allows attackers to cause a denial of service (application crash) via a crafted input.   |
| Git | 2.45.2 | CVE-2022-1698  | HIGH                 | 7.5        | Allowing long password leads to denial of service in GitHub repository causefx/organizr prior to 2.1.2000. This vulnerability can be abused by doing a DDoS attack for which genuine users will not be able to access resources/applications.  |
| Git | 2.45.2 | CVE-2022-1699  | HIGH                 | 7.5        | Uncontrolled Resource Consumption in GitHub repository causefx/organizr prior to 2.1.2000. This vulnerability can be abused by doing a DDoS attack for which genuine users will not be able to access resources/applications.  |
| Git | 2.45.2 | CVE-2022-1714  | HIGH                 | 7.1        | Out-of-bounds Read in GitHub repository radareorg/radare2 prior to 5.7.0. The bug causes the program to read data past the end of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.   |
| Git | 2.45.2 | CVE-2022-1715  | CRITICAL             | 9.8        | Account Takeover in GitHub repository neorazorx/facturascripts prior to 2022.07.   |
| Git | 2.45.2 | CVE-2022-25865 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | The package workspace-tools before 0.18.4 are vulnerable to Command Injection via git argument injection. When calling the fetchRemoteBranch(remote: string, remoteBranch: string, cwd: string) function, both the remote and remoteBranch parameters are passed to the git fetch subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection. |
| Git | 2.45.2 | CVE-2022-1379  | CRITICAL             | 9.1        | URL Restriction Bypass in GitHub repository plantuml/plantuml prior to V1.2022.5. An attacker can abuse this to bypass URL restrictions that are imposed by the different security profiles and achieve server side request forgery (SSRF). This allows accessing restricted internal resources/servers or sending requests to third party servers.  |
| Git | 2.45.2 | CVE-2022-30781 | HIGH                 | 7.5        | Gitea before 1.16.7 does not escape git fetch remote.  |
| Git | 2.45.2 | CVE-2022-0574  | MEDIUM               | 6.5        | Improper Access Control in GitHub repository publify/publify prior to 9.2.8.   |
| Git | 2.45.2 | CVE-2022-0578  | MEDIUM               | 6.5        | Code Injection in GitHub repository publify/publify prior to 9.2.8.  |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2022-1553  | MEDIUM | 4.9 | Leaking password protected articles content due to improper access control in GitHub repository publi/publish prior to 9.2.8. Attackers can leverage this vulnerability to view the contents of any password-protected article present on the publi website, compromising confidentiality and integrity of users. |
| Git | 2.45.2 | CVE-2022-1713  | HIGH   | 7.5 | SSRF on /proxy in GitHub repository jgraph/drawio prior to 18.0.4. An attacker can make a request as the server and read its contents. This can lead to a leak of sensitive information.  |
| Git | 2.45.2 | CVE-2022-1721  | HIGH   | 7.5 | Path Traversal in WellKnownServlet in GitHub repository jgraph/drawio prior to 18.0.5. Read local files of the web application.   |
| Git | 2.45.2 | CVE-2022-1722  | LOW    | 3.3 | SSRF in editor's proxy via IPv6 link-local address in GitHub repository jgraph/drawio prior to 18.0.5. SSRF to internal link-local IPv6 addresses   |
| Git | 2.45.2 | CVE-2022-1726  | MEDIUM | 5.4 | Bootstrap Tables XSS vulnerability with Table Export plug-in when exportOptions: htmlContent is true in GitHub repository wenzhixin/bootstrap-table prior to 1.20.2. Disclosing session cookies, disclosing secure session data, exfiltrating data to third-parties.  |
| Git | 2.45.2 | CVE-2022-1728  | MEDIUM | 6.5 | Allowing long password leads to denial of service in polonel/trudesk in GitHub repository polonel/trudesk prior to 1.2.2. This vulnerability can be abused by doing a DDoS attack for which genuine users will not be able to access resources/applications.  |
| Git | 2.45.2 | CVE-2022-1723  | HIGH   | 7.5 | Server-Side Request Forgery (SSRF) in GitHub repository jgraph/drawio prior to 18.0.6.  |
| Git | 2.45.2 | CVE-2022-1711  | HIGH   | 7.5 | Server-Side Request Forgery (SSRF) in GitHub repository jgraph/drawio prior to 18.0.5.  |
| Git | 2.45.2 | CVE-2022-30947 | HIGH   | 7.5 | Jenkins Git Plugin 4.11.1 and earlier allows attackers able to configure pipelines to check out some SCM repositories stored on the Jenkins controller's file system using local paths as SCM URLs, obtaining limited information about other projects' SCM contents.   |
| Git | 2.45.2 | CVE-2022-30955 | MEDIUM | 6.5 | Jenkins GitLab Plugin 1.5.31 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.  |
| Git | 2.45.2 | CVE-2022-1733  | HIGH   | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.4968.  |
| Git | 2.45.2 | CVE-2022-1769  | HIGH   | 7.8 | Buffer Over-read in GitHub repository vim/vim prior to 8.2.4974.  |

|     |        |               |                      |            |   |
|-----|--------|---------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1735 | HIGH                 | 7.8        | Classic Buffer Overflow in GitHub repository vim/vim prior to 8.2.4969.   |
| Git | 2.45.2 | CVE-2022-1430 | HIGH                 | 7.5        | Cross-site Scripting (XSS) - DOM in GitHub repository octoprint/octoprint prior to 1.8.0.   |
| Git | 2.45.2 | CVE-2022-1432 | MEDIUM               | 6.4        | Cross-site Scripting (XSS) - Generic in GitHub repository octoprint/octoprint prior to 1.8.0.   |
| Git | 2.45.2 | CVE-2022-1727 | HIGH                 | 8.8        | Improper Input Validation in GitHub repository jgraph/drawio prior to 18.0.6.   |
| Git | 2.45.2 | CVE-2022-1782 | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Generic in GitHub repository erudika/para prior to v1.45.11.   |
| Git | 2.45.2 | CVE-2022-1795 | CRITICAL             | 9.8        | Use After Free in GitHub repository gpac/gpac prior to v2.1.0-DEV.  |
| Git | 2.45.2 | CVE-2022-1767 | HIGH                 | 7.5        | Server-Side Request Forgery (SSRF) in GitHub repository jgraph/drawio prior to 18.0.7.  |
| Git | 2.45.2 | CVE-2022-1771 | MEDIUM               | 5.5        | Uncontrolled Recursion in GitHub repository vim/vim prior to 8.2.4975.  |
| Git | 2.45.2 | CVE-2022-1774 | MEDIUM               | 6.1        | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository jgraph/drawio prior to 18.0.7.  |
| Git | 2.45.2 | CVE-2022-1785 | HIGH                 | 7.8        | Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.4977.   |
| Git | 2.45.2 | CVE-2022-1730 | MEDIUM               | 4.6        | Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 18.0.4.   |
| Git | 2.45.2 | CVE-2022-1796 | HIGH                 | 7.8        | Use After Free in GitHub repository vim/vim prior to 8.2.4979.  |
| Git | 2.45.2 | CVE-2022-1413 | ['MEDIUM', 'HIGH']   | [5.4, 7.5] | Missing input masking in GitLab CE/EE affecting all versions starting from 1.0.2 before 14.8.6, all versions from 14.9.0 before 14.9.4, and all versions from 14.10.0 before 14.10.1 causes potentially sensitive integration properties to be disclosed in the web interface   |
| Git | 2.45.2 | CVE-2022-1416 | ['MEDIUM', 'MEDIUM'] | [4.3, 5.4] | Missing sanitization of data in Pipeline error messages in GitLab CE/EE affecting all versions starting from 1.0.2 before 14.8.6, all versions from 14.9.0 before 14.9.4, and all versions from 14.10.0 before 14.10.1 allows for rendering of attacker controlled HTML tags and CSS styling  |
| Git | 2.45.2 | CVE-2022-1423 | ['HIGH', 'HIGH']     | [7.1, 8.8] | Improper access control in the CI/CD cache mechanism in GitLab CE/EE affecting all versions starting from 1.0.2 before 14.8.6, all versions from 14.9.0 before 14.9.4, and all versions from 14.10.0 before 14.10.1 allows a malicious actor with Developer privileges to perform cache poisoning leading to arbitrary code execution in protected branches |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1754  | MEDIUM               | 6.5        | Integer Overflow or Wraparound in GitHub repository polonel/trudesk prior to 1.2.2.   |
| Git | 2.45.2 | CVE-2022-1806  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository rtxteam/rtx prior to checkpoint_2022-05-18.   |
| Git | 2.45.2 | CVE-2022-1784  | HIGH                 | 7.5        | Server-Side Request Forgery (SSRF) in GitHub repository jgraph/drawio prior to 18.0.8.  |
| Git | 2.45.2 | CVE-2022-24904 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 0.7.0 and prior to versions 2.1.15m 2.2.9, and 2.3.4 is vulnerable to a symlink following bug allowing a malicious user with repository write access to leak sensitive files from Argo CD's repo-server. A malicious Argo CD user with write access for a repository which is (or may be) used in a directory-type Application may commit a symlink which points to an out-of-bounds file. Sensitive files which could be leaked include manifest files from other Applications' source repositories (potentially decrypted files, if you are using a decryption plugin) or any JSON-formatted secrets which have been mounted as files on the repo-server. A patch for this vulnerability has been released in Argo CD versions 2.3.4, 2.2.9, and 2.1.15. Users of versions 2.3.0 or above who do not have any Jsonnet/directory-type Applications may disable the Jsonnet/directory config management tool as a workaround. |
| Git | 2.45.2 | CVE-2022-24905 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. A vulnerability was found in Argo CD prior to versions 2.3.4, 2.2.9, and 2.1.15 that allows an attacker to spoof error messages on the login screen when single sign on (SSO) is enabled. In order to exploit this vulnerability, an attacker would have to trick the victim to visit a specially crafted URL which contains the message to be displayed. As far as the research of the Argo CD team concluded, it is not possible to specify any active content (e.g. Javascript) or other HTML fragments (e.g. clickable links) in the spoofed message. A patch for this vulnerability has been released in Argo CD versions 2.3.4, 2.2.9, and 2.1.15. There are currently no known workarounds.  |

|     |        |                |                          |              |  |
|-----|--------|----------------|--------------------------|--------------|--|
| Git | 2.45.2 | CVE-2022-29165 | ['CRITICAL', 'CRITICAL'] | [10.0, 10.0] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. A critical vulnerability has been discovered in Argo CD starting with version 1.4.0 and prior to versions 2.1.15, 2.2.9, and 2.3.4 which would allow unauthenticated users to impersonate as any Argo CD user or role, including the `admin` user, by sending a specifically crafted JSON Web Token (JWT) along with the request. In order for this vulnerability to be exploited, anonymous access to the Argo CD instance must have been enabled. In a default Argo CD installation, anonymous access is disabled. The vulnerability can be exploited to impersonate as any user or role, including the built-in `admin` account regardless of whether it is enabled or disabled. Also, the attacker does not need an account on the Argo CD instance in order to exploit this. If anonymous access to the instance is enabled, an attacker can escalate their privileges, effectively allowing them to gain the same privileges on the cluster as the Ar... |
| Git | 2.45.2 | CVE-2022-1770  | HIGH                     | 8.8          | Improper Privilege Management in GitHub repository polonel/trudesk prior to 1.2.2.   |
| Git | 2.45.2 | CVE-2022-29178 | ['HIGH', 'HIGH']         | [8.8, 8.2]   | Cilium is open source software for providing and securing network connectivity and loadbalancing between application workloads. Cilium prior to versions 1.9.16, 1.10.11, and 1.11.15 contains an incorrect default permissions vulnerability. Operating Systems with users belonging to the group ID 1000 can access the API of Cilium via Unix domain socket available on the host where Cilium is running. This could allow malicious users to compromise integrity as well as system availability on that host. The problem has been fixed and the patch is available in versions 1.9.16, 1.10.11, and 1.11.5. A potential workaround is to modify Cilium's DaemonSet to run with a certain command, which can be found in the GitHub Security Advisory for this vulnerability.  |
| Git | 2.45.2 | CVE-2022-1803  | MEDIUM                   | 6.9          | Improper Restriction of Rendered UI Layers or Frames in GitHub repository polonel/trudesk prior to 1.2.2.  |
| Git | 2.45.2 | CVE-2022-1775  | CRITICAL                 | 9.8          | Weak Password Requirements in GitHub repository polonel/trudesk prior to 1.2.2.  |
| Git | 2.45.2 | CVE-2022-1752  | HIGH                     | 8.0          | Unrestricted Upload of File with Dangerous Type in GitHub repository polonel/trudesk prior to 1.2.2.   |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-31267 | CRITICAL           | 9.8        | Gitblit 1.9.2 allows privilege escalation via the Config User Service: a control character can be placed in a profile data field, such as an emailAddress%3Atext 'attacker@example.com\n\trol e = "#admin"' value.   |
| Git | 2.45.2 | CVE-2022-31268 | HIGH               | 7.5        | A Path Traversal vulnerability in Gitblit 1.9.3 can lead to reading website files via /resources/./ (e.g., followed by a WEB-INF or META-INF pathname).  |
| Git | 2.45.2 | CVE-2022-1809  | HIGH               | 7.8        | Access of Uninitialized Pointer in GitHub repository radareorg/radare2 prior to 5.7.0.   |
| Git | 2.45.2 | CVE-2022-1813  | CRITICAL           | 9.8        | OS Command Injection in GitHub repository yogeshojha/engine prior to 1.2.0.  |
| Git | 2.45.2 | CVE-2022-1825  | MEDIUM             | 5.4        | Cross-site Scripting (XSS) - Reflected in GitHub repository collectiveaccess/providence prior to 1.8.  |
| Git | 2.45.2 | CVE-2022-1810  | MEDIUM             | 4.3        | Authorization Bypass Through User-Controlled Key in GitHub repository publify/publify prior to 9.2.9.  |
| Git | 2.45.2 | CVE-2022-1811  | MEDIUM             | 5.4        | Unrestricted Upload of File with Dangerous Type in GitHub repository publify/publify prior to 9.2.9.   |
| Git | 2.45.2 | CVE-2022-1848  | MEDIUM             | 5.3        | Business Logic Errors in GitHub repository erudika/para prior to 1.45.11.  |
| Git | 2.45.2 | CVE-2022-1850  | HIGH               | 8.1        | Path Traversal in GitHub repository filegator/filegator prior to 7.8.0.  |
| Git | 2.45.2 | CVE-2022-1849  | MEDIUM             | 5.4        | Session Fixation in GitHub repository filegator/filegator prior to 7.8.0.  |
| Git | 2.45.2 | CVE-2022-1815  | HIGH               | 7.5        | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository jgraph/drawio prior to 18.1.2.   |
| Git | 2.45.2 | CVE-2022-1883  | HIGH               | 8.8        | SQL Injection in GitHub repository camptocamp/terraboard prior to 2.2.0.   |
| Git | 2.45.2 | CVE-2022-1851  | HIGH               | 7.8        | Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-29251 | ['HIGH', 'MEDIUM'] | [7.4, 6.1] | XWiki Platform Flamingo Theme UI is a tool that allows customization and preview of any Flamingo-based skin. Starting with versions 6.2.4 and 6.3-rc-1, a possible cross-site scripting vector is present in the `FlamingoThemesCode.WebHomeSheet` wiki page related to the "newThemeName" form field. The issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3. The easiest available workaround is to edit the wiki page `FlamingoThemesCode.WebHomeSheet` (with wiki editor) according to the suggestion provided in the GitHub Security Advisory. |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-29252 | ['HIGH', 'MEDIUM'] | [7.4, 6.1] | XWiki Platform Wiki UI Main Wiki is a package for managing subwikis. Starting with version 5.3-milestone-2, XWiki Platform Wiki UI Main Wiki contains a possible cross-site scripting vector in the `WikiManager.JoinWiki` wiki page related to the "requestJoin" field. The issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3. The easiest available workaround is to edit the wiki page `WikiManager.JoinWiki` (with wiki editor) according to the suggestion provided in the GitHub Security Advisory. |
| Git | 2.45.2 | CVE-2022-1886  | HIGH               | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-1899  | CRITICAL           | 9.1        | Out-of-bounds Read in GitHub repository radareorg/radare2 prior to 5.7.0.   |
| Git | 2.45.2 | CVE-2022-1898  | HIGH               | 7.8        | Use After Free in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-1907  | HIGH               | 8.1        | Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11.   |
| Git | 2.45.2 | CVE-2022-1908  | HIGH               | 8.1        | Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11.   |
| Git | 2.45.2 | CVE-2022-1909  | MEDIUM             | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository causefx/organizr prior to 2.1.2200.  |
| Git | 2.45.2 | CVE-2022-1897  | HIGH               | 7.8        | Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-1927  | HIGH               | 7.8        | Buffer Over-read in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-1928  | MEDIUM             | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository go-gitea/gitea prior to 1.16.9.  |
| Git | 2.45.2 | CVE-2022-1931  | HIGH               | 8.1        | Incorrect Synchronization in GitHub repository polonel/trudesk prior to 1.2.3.  |
| Git | 2.45.2 | CVE-2022-1934  | HIGH               | 7.8        | Use After Free in GitHub repository mruby/mruby prior to 3.2.   |
| Git | 2.45.2 | CVE-2022-1926  | MEDIUM             | 4.9        | Integer Overflow or Wraparound in GitHub repository polonel/trudesk prior to 1.2.3.   |
| Git | 2.45.2 | CVE-2022-1942  | HIGH               | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-29220 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | github-action-merge-dependabot is an action that automatically approves and merges dependabot pull requests (PRs). Prior to version 3.2.0, github-action-merge-dependabot does not check if a commit created by dependabot is verified with the proper GPG key. There is just a check if the actor is set to `dependabot[bot]` to determine if the PR is a legit PR. Theoretically, an owner of a seemingly valid and legit action in the pipeline can check if the PR is created by dependabot and if their own action has enough permissions to modify the PR in the pipeline. If so, they can modify the PR by adding a second seemingly valid and legit commit to the PR, as they can set arbitrarily the username and email in for commits in git. Because the bot only checks if the actor is valid, it would pass the malicious changes through and merge the PR automatically, without getting noticed by project maintainers. It would probably not be possible to determine where the malicious commit came from, as it wou... |
| Git | 2.45.2 | CVE-2022-29258 | ['HIGH', 'MEDIUM']   | [7.4, 6.1] | XWiki Platform Filter UI provides a generic user interface to convert from a XWiki Filter input stream to an output stream with settings for each stream. Starting with versions 6.0-milestone-2 and 5.4.4 and prior to versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3, XWiki Platform Filter UI contains a possible cross-site scripting vector in the `Filter.FilterStreamDescriptorForm` wiki page related to pretty much all the form fields printed in the home page of the application. The issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, and 13.10.3. The easiest workaround is to edit the wiki page `Filter.FilterStreamDescriptorForm` (with wiki editor) according to the instructions in the GitHub Security Advisory.  |
| Git | 2.45.2 | CVE-2022-1808  | HIGH                 | 8.8        | Execution with Unnecessary Privileges in GitHub repository polonel/trudesk prior to 1.2.3.   |
| Git | 2.45.2 | CVE-2022-1893  | ['MEDIUM', 'MEDIUM'] | [4.6, 5.3] | Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository polonel/trudesk prior to 1.2.3.  |
| Git | 2.45.2 | CVE-2022-1947  | MEDIUM               | 6.5        | Use of Incorrect Operator in GitHub repository polonel/trudesk prior to 1.2.3.   |
| Git | 2.45.2 | CVE-2022-1285  | MEDIUM               | 6.5        | Server-Side Request Forgery (SSRF) in GitHub repository gogs/gogs prior to 0.12.8.   |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2022-24848 | ['HIGH', 'HIGH'] | [8.8, 8.8] | DHIS2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability affects the <code>`/api/programs/orgUnits?programs=`</code> API endpoint in DHIS2 versions prior to 2.36.10.1 and 2.37.6.1. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. The vulnerability is not exposed to a non-malicious user and requires a conscious attack to be exploited. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance's database. Security patches are now available for DHIS2 versions 2.36.10.1 and 2.37.6.1. One may apply mitigations at the web proxy level as a workaround. More information about these mitigations is available in the GitHub Security Advisory. |
| Git | 2.45.2 | CVE-2022-29169 | ['HIGH', 'HIGH'] | [7.5, 7.5] | BigBlueButton is an open source web conferencing system. Versions starting with 2.2 and prior to 2.3.19, 2.4.7, and 2.5.0-beta.2 are vulnerable to regular expression denial of service (ReDoS) attacks. By using specific a RegularExpression, an attacker can cause denial of service for the bbb-html5 service. The useragent library performs checking of device by parsing the input of User-Agent header and lets it go through <code>lookupUserAgent()</code> (alias of <code>useragent.lookup()</code> ). This function handles input by regexing and attackers can abuse that by providing some ReDos payload using <code>`SmartWatch`</code> . The maintainers removed <code>`htmlclient/useragent`</code> from versions 2.3.19, 2.4.7, and 2.5.0-beta.2. As a workaround, disable NginX forwarding the requests to the handler according to the directions in the GitHub Security Advisory.   |
| Git | 2.45.2 | CVE-2021-32546 | HIGH             | 8.8        | Missing input validation in <code>internal/db/repo_editor.go</code> in Gogs before 0.12.8 allows an attacker to execute code remotely. An unprivileged attacker (registered user) can overwrite the Git configuration in his repository. This leads to Remote Command Execution, because that configuration can contain an option such as <code>sshCommand</code> , which is executed when a master branch is a remote branch (using an <code>ssh://URI</code> ). The remote branch can also be configured by editing the Git configuration file. One can create a new file in a new repository, using the GUI, with <code>"\"</code> as its name, and then rename this file to <code>.git/config</code> with the custom configuration content (and then save it).   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2021-34081 | HIGH                 | 8.8        | OS Command Injection vulnerability in bbultman gitsome through 0.2.3 allows attackers to execute arbitrary commands via a crafted tag name of the target git repository.   |
| Git | 2.45.2 | CVE-2022-1968  | HIGH                 | 7.8        | Use After Free in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-1987  | HIGH                 | 8.1        | Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11.  |
| Git | 2.45.2 | CVE-2022-1988  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Generic in GitHub repository neorazorx/facturascripts prior to 2022.09.   |
| Git | 2.45.2 | CVE-2021-39947 | ['MEDIUM', 'HIGH']   | [5.3, 7.5] | In specific circumstances, trace file buffers in GitLab Runner versions up to 14.3.4, 14.4 to 14.4.2, and 14.5 to 14.5.2 would re-use the file descriptor 0 for multiple traces and mix the output of several jobs   |
| Git | 2.45.2 | CVE-2022-1783  | ['LOW', 'LOW']       | [2.7, 2.7] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.3 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. It may be possible for malicious group maintainers to add new members to a project within their group, through the REST API, even after their group owner enabled a setting to prevent members from being added to projects within that group. |
| Git | 2.45.2 | CVE-2022-1821  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.8 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. It may be possible for a subgroup member to access the members list of their parent group.   |
| Git | 2.45.2 | CVE-2022-1935  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Trigger Token to misuse it from any location even when IP address restrictions were configured  |
| Git | 2.45.2 | CVE-2022-1936  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Deploy Token to misuse it from any location even when IP address restrictions were configured   |

|     |        |               |                      |            |   |
|-----|--------|---------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-1940 | ['HIGH', 'MEDIUM']   | [7.7, 5.4] | A Stored Cross-Site Scripting vulnerability in Jira integration in GitLab EE affecting all versions from 13.11 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1 allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf via specially crafted Jira Issues   |
| Git | 2.45.2 | CVE-2022-1944 | ['MEDIUM', 'HIGH']   | [5.4, 7.1] | When the feature is configured, improper authorization in the Interactive Web Terminal in GitLab CE/EE affecting all versions from 11.3 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1 allows users with the Developer role to open terminals on other Developers' running jobs  |
| Git | 2.45.2 | CVE-2022-1680 | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | An account takeover issue has been discovered in GitLab EE affecting all versions starting from 11.10 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. When group SAML SSO is configured, the SCIM feature (available only on Premium+ subscriptions) may allow any owner of a Premium group to invite arbitrary users through their username and email, then change those users' email addresses via SCIM to an attacker controlled email address and thus - in the absence of 2FA - take over those accounts. It is also possible for the attacker to change the display name and username of the targeted account. |
| Git | 2.45.2 | CVE-2022-2022 | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository nocodb/nocodb prior to 0.91.7.   |
| Git | 2.45.2 | CVE-2022-1996 | CRITICAL             | 9.1        | Authorization Bypass Through User-Controlled Key in GitHub repository emicklei/go-restful prior to v3.8.0.  |
| Git | 2.45.2 | CVE-2022-1997 | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 9.0.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-31027 | ['MEDIUM', 'MEDIUM'] | [4.2, 6.5] | OAuthenticator is an OAuth token library for the JupyterHub login handler. CILogonOAuthenticator is provided by the OAuthenticator package, and lets users log in to a JupyterHub via CILogon. This is primarily used to restrict a JupyterHub only to users of a given institute. The allowed_idps configuration trait of CILogonOAuthenticator is documented to be a list of domains that indicate the institutions whose users are authorized to access this JupyterHub. This authorization is validated by ensuring that the *email* field provided to us by CILogon has a *domain* that matches one of the domains listed in `allowed_idps`. If `allowed_idps` contains `berkeley.edu`, you might expect only users with valid current credentials provided by University of California, Berkeley to be able to access the JupyterHub. However, CILogonOAuthenticator does *not* verify which provider is used by the user to login, only the email address provided. So a user can login with a GitHub account that has email set... |
| Git | 2.45.2 | CVE-2022-2000  | HIGH                 | 7.8        | Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2016  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Reflected in GitHub repository neorazorx/facturascripts prior to 2022.1.  |
| Git | 2.45.2 | CVE-2022-1986  | CRITICAL             | 9.8        | OS Command Injection in GitHub repository gogs/gogs prior to 0.12.9.   |
| Git | 2.45.2 | CVE-2022-1992  | CRITICAL             | 9.1        | Path Traversal in GitHub repository gogs/gogs prior to 0.12.9.   |
| Git | 2.45.2 | CVE-2022-1993  | HIGH                 | 8.1        | Path Traversal in GitHub repository gogs/gogs prior to 0.12.9.   |
| Git | 2.45.2 | CVE-2022-2014  | MEDIUM               | 5.4        | Code Injection in GitHub repository jgraph/drawio prior to 19.0.2.   |
| Git | 2.45.2 | CVE-2022-2015  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 19.0.2.  |
| Git | 2.45.2 | CVE-2022-2026  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository kromitgmbh/titra prior to 0.77.0.   |
| Git | 2.45.2 | CVE-2022-2027  | HIGH                 | 8.0        | Improper Neutralization of Formula Elements in a CSV File in GitHub repository kromitgmbh/titra prior to 0.77.0.   |
| Git | 2.45.2 | CVE-2022-2028  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Generic in GitHub repository kromitgmbh/titra prior to 0.77.0.  |
| Git | 2.45.2 | CVE-2022-2029  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - DOM in GitHub repository kromitgmbh/titra prior to 0.77.0.  |
| Git | 2.45.2 | CVE-2022-2036  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 9.0.1.  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-2037  | HIGH                 | 8.0        | Excessive Attack Surface in GitHub repository tooljet/tooljet prior to v1.16.0.   |
| Git | 2.45.2 | CVE-2022-31038 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | Gogs is an open source self-hosted Git service. In versions of gogs prior to 0.12.9 `DisplayName` does not filter characters input from users, which leads to an XSS vulnerability when directly displayed in the issue list. This issue has been resolved in commit 155cae1d which sanitizes `DisplayName` prior to display to the user. All users of gogs are advised to upgrade. Users unable to upgrade should check their users' display names for malicious characters. |
| Git | 2.45.2 | CVE-2022-2042  | HIGH                 | 7.8        | Use After Free in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-24376 | ['HIGH', 'CRITICAL'] | [7.2, 9.8] | All versions of package git-promise are vulnerable to Command Injection due to an inappropriate fix of a prior [vulnerability](https://security.snyk.io/vuln/SNYK-JS-GITPROMISE-567476) in this package.<br>**Note:** Please note that the vulnerability will not be fixed. The README file was updated with a warning regarding this issue.  |
| Git | 2.45.2 | CVE-2022-2054  | ['HIGH', 'HIGH']     | [8.4, 7.8] | Code Injection in GitHub repository nuitka/nuitka prior to 0.9.   |
| Git | 2.45.2 | CVE-2022-2060  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository dolibarr/dolibarr prior to 16.0.   |
| Git | 2.45.2 | CVE-2022-2061  | LOW                  | 3.3        | Heap-based Buffer Overflow in GitHub repository hpjansson/chafa prior to 1.12.0.  |
| Git | 2.45.2 | CVE-2022-2062  | HIGH                 | 7.5        | Generation of Error Message Containing Sensitive Information in GitHub repository nocodb/nocodb prior to 0.91.7+.   |
| Git | 2.45.2 | CVE-2022-2063  | HIGH                 | 8.8        | Improper Privilege Management in GitHub repository nocodb/nocodb prior to 0.91.7+.  |
| Git | 2.45.2 | CVE-2022-2064  | HIGH                 | 8.8        | Insufficient Session Expiration in GitHub repository nocodb/nocodb prior to 0.91.7+.  |
| Git | 2.45.2 | CVE-2022-2065  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository neorazorx/facturascripts prior to 2022.06.   |
| Git | 2.45.2 | CVE-2022-2066  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository neorazorx/facturascripts prior to 2022.06.  |
| Git | 2.45.2 | CVE-2022-2067  | CRITICAL             | 9.1        | SQL Injection in GitHub repository francoisjacquet/rosariosis prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2079  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository nocodb/nocodb prior to 0.91.7+.  |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-31066 | ['MEDIUM', 'MEDIUM'] | [5.9, 4.4] | <p>EdgeX Foundry is an open source project for building a common open framework for Internet of Things edge computing. Prior to version 2.1.1, the /api/v2/config endpoint exposes message bus credentials to local unauthenticated users. In security-enabled mode, message bus credentials are supposed to be kept in the EdgeX secret store and require authentication to access. This vulnerability bypasses the access controls on message bus credentials when running in security-enabled mode. (No credentials are required when running in security-disabled mode.) As a result, attackers could intercept data or inject fake data into the EdgeX message bus. Users should upgrade to EdgeX Foundry Kamakura release (2.2.0) or to the June 2022 EdgeX Foundry LTS Jakarta release (2.1.1) to receive a patch. More information about which go modules, docker containers, and snaps contain patches is available in the GitHub Security Advisory. There are currently no known workarounds for this issue.</p>               |
| Git | 2.45.2 | CVE-2022-31069 | ['MEDIUM', 'HIGH']   | [5.8, 7.5] | <p>NestJS Proxy is a NestJS module to decorate and proxy calls. Prior to version 0.7.0, the nestjs-proxy library did not have a way to control when Authorization headers should be forwarded for specific backend services configured by the application developer. This could have resulted in sensitive information such as OAuth bearer access tokens being inadvertently exposed to such services that should not see them. A new feature has been introduced in the patched version of nestjs-proxy that allows application developers to opt out of forwarding the Authorization headers on a per service basis using the `forwardToken` config setting. Developers are advised to review the README for this library on Github or NPM for further details on how this configuration can be applied. This issue has been fixed in version 0.7.0 of `@finastra/nestjs-proxy`. Users of `@ffdc/nestjs-proxy` are advised that this package has been deprecated and is no longer being maintained or receiving updates. Such ...</p> |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2022-31072 | ['LOW', 'LOW']   | [2.5, 3.3] | Octokit is a Ruby toolkit for the GitHub API. Versions 4.23.0 and 4.24.0 of the octokit gem were published containing world-writable files. Specifically, the gem was packed with files having their permissions set to <code>-rw-rw-rw-</code> (i.e. 0666) instead of <code>-rw-r--r--</code> (i.e. 0644). This means everyone who is not the owner (Group and Public) with access to the instance where this release had been installed could modify the world-writable files from this gem. This issue is patched in Octokit 4.25.0. Two workarounds are available. Users can use the previous version of the gem, v4.22.0. Alternatively, users can modify the file permissions manually until they are able to upgrade to the latest version. |
| Git | 2.45.2 | CVE-2022-2098  | CRITICAL         | 9.8        | Weak Password Requirements in GitHub repository kromitgmbh/titra prior to 0.78.1.  |
| Git | 2.45.2 | CVE-2022-2111  | HIGH             | 8.8        | Unrestricted Upload of File with Dangerous Type in GitHub repository inventree/inventree prior to 0.7.2.   |
| Git | 2.45.2 | CVE-2022-2112  | HIGH             | 8.8        | Improper Neutralization of Formula Elements in a CSV File in GitHub repository inventree/inventree prior to 0.7.2.   |
| Git | 2.45.2 | CVE-2022-2113  | MEDIUM           | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository inventree/inventree prior to 0.7.2.   |
| Git | 2.45.2 | CVE-2022-25856 | ['HIGH', 'HIGH'] | [7.5, 7.5] | The package github.com/argoproj/argo-events/sensors/artifacts before 1.7.1 are vulnerable to Directory Traversal in the (g *GitArtifactReader).Read() API in git.go. This could allow arbitrary file reads if the GitArtifactReader is provided a pathname containing a symbolic link or an implicit directory name such as ..   |
| Git | 2.45.2 | CVE-2022-2124  | HIGH             | 7.8        | Buffer Over-read in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-2125  | HIGH             | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-2126  | HIGH             | 7.8        | Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.  |
| Git | 2.45.2 | CVE-2022-2129  | HIGH             | 7.8        | Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2023  | CRITICAL         | 9.8        | Incorrect Use of Privileged APIs in GitHub repository polonel/trudesk prior to 1.2.4.  |
| Git | 2.45.2 | CVE-2022-2130  | MEDIUM           | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.17.   |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2022-1720  | HIGH     | 7.8 | Buffer Over-read in function grab_file_name in GitHub repository vim/vim prior to 8.2.4956. This vulnerability is capable of crashing the software, memory modification, and possible remote execution. |
| Git | 2.45.2 | CVE-2022-2134  | MEDIUM   | 6.5 | Allocation of Resources Without Limits or Throttling in GitHub repository inventree/inventree prior to 0.8.0.   |
| Git | 2.45.2 | CVE-2022-2128  | CRITICAL | 9.8 | Unrestricted Upload of File with Dangerous Type in GitHub repository polonel/trudesk prior to 1.2.4.  |
| Git | 2.45.2 | CVE-2022-2174  | MEDIUM   | 6.1 | Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.18.  |
| Git | 2.45.2 | CVE-2022-2175  | HIGH     | 7.8 | Buffer Over-read in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2182  | HIGH     | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2183  | HIGH     | 7.8 | Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2206  | HIGH     | 7.8 | Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2021-40899 | HIGH     | 7.5 | A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in repo-git-downloader v0.1.1 when downloading crafted invalid git repositories.  |
| Git | 2.45.2 | CVE-2022-0722  | HIGH     | 7.5 | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository ionicabizau/parse-url prior to 7.0.0.   |
| Git | 2.45.2 | CVE-2022-2217  | MEDIUM   | 6.1 | Cross-site Scripting (XSS) - Generic in GitHub repository ionicabizau/parse-url prior to 7.0.0.   |
| Git | 2.45.2 | CVE-2022-2207  | HIGH     | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2216  | CRITICAL | 9.8 | Server-Side Request Forgery (SSRF) in GitHub repository ionicabizau/parse-url prior to 7.0.0.   |
| Git | 2.45.2 | CVE-2022-2208  | MEDIUM   | 5.5 | NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.5163.  |
| Git | 2.45.2 | CVE-2022-2218  | MEDIUM   | 6.1 | Cross-site Scripting (XSS) - Stored in GitHub repository ionicabizau/parse-url prior to 7.0.0.  |
| Git | 2.45.2 | CVE-2022-2210  | HIGH     | 7.8 | Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.  |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2022-31034 | ['HIGH', 'HIGH']       | [8.3, 8.1] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v0.11.0 are vulnerable to a variety of attacks when an SSO login is initiated from the Argo CD CLI or UI. The vulnerabilities are due to the use of insufficiently random values in parameters in OAuth2/OIDC login flows. In each case, using a relatively-predictable (time-based) seed in a non-cryptographically-secure pseudo-random number generator made the parameter less random than required by the relevant spec or by general best practices. In some cases, using too short a value made the entropy even less sufficient. The attacks on login flows which are meant to be mitigated by these parameters are difficult to accomplish but can have a high impact potentially granting an attacker admin access to Argo CD. Patches for this vulnerability has been released in the following Argo CD versions: v2.4.1, v2.3.5, v2.2.10 and v2.1.16. There are no known workarounds for this vulnerability. |
| Git | 2.45.2 | CVE-2022-31035 | ['CRITICAL', 'MEDIUM'] | [9.0, 5.4] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v1.0.0 are vulnerable to a cross-site scripting (XSS) bug allowing a malicious user to inject a `javascript:` link in the UI. When clicked by a victim user, the script will execute with the victim's permissions (up to and including admin). The script would be capable of doing anything which is possible in the UI or via the API, such as creating, modifying, and deleting Kubernetes resources. A patch for this vulnerability has been released in the following Argo CD versions: v2.4.1, v2.3.5, v2.2.10 and v2.1.16. There are no completely-safe workarounds besides upgrading.   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-31036 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v1.3.0 are vulnerable to a symlink following bug allowing a malicious user with repository write access to leak sensitive YAML files from Argo CD's repo-server. A malicious Argo CD user with write access for a repository which is (or may be) used in a Helm-type Application may commit a symlink which points to an out-of-bounds file. If the target file is a valid YAML file, the attacker can read the contents of that file. Sensitive files which could be leaked include manifest files from other Applications' source repositories (potentially decrypted files, if you are using a decryption plugin) or any YAML-formatted secrets which have been mounted as files on the repo-server. Patches for this vulnerability has been released in the following Argo CD versions: v2.4.1, v2.3.5, v2.2.10 and v2.1.16. If you are using a version >=v2.3.0 and do not have any Helm-type Applications you ...  |
| Git | 2.45.2 | CVE-2022-31098 | ['CRITICAL', 'HIGH'] | [9.0, 7.5] | Weave GitOps is a simple open source developer platform for people who want cloud native applications, without needing Kubernetes expertise. A vulnerability in the logging of Weave GitOps could allow an authenticated remote attacker to view sensitive cluster configurations, aka KubeConfig, of registered Kubernetes clusters, including the service account tokens in plain text from Weave GitOps's pod logs on the management cluster. An unauthorized remote attacker can also view these sensitive configurations from external log storage if enabled by the management cluster. This vulnerability is due to the client factory dumping cluster configurations and their service account tokens when the cluster manager tries to connect to an API server of a registered cluster, and a connection error occurs. An attacker could exploit this vulnerability by either accessing logs of a pod of Weave GitOps, or from external log storage and obtaining all cluster configurations of registered clusters. A succe... |
| Git | 2.45.2 | CVE-2022-0624  | HIGH                 | 7.3        | Authorization Bypass Through User-Controlled Key in GitHub repository ionicabizau/parse-path prior to 5.0.0.  |
| Git | 2.45.2 | CVE-2022-0085  | MEDIUM               | 5.3        | Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.   |
| Git | 2.45.2 | CVE-2022-2231  | MEDIUM               | 5.5        | NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.   |
| Git | 2.45.2 | CVE-2022-2252  | MEDIUM               | 6.1        | Open Redirect in GitHub repository microweber/microweber prior to 1.2.19.   |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-2073  | HIGH                 | 7.2        | Code Injection in GitHub repository getgrav/grav prior to 1.7.34.  |
| Git | 2.45.2 | CVE-2022-34777 | MEDIUM               | 5.4        | Jenkins GitLab Plugin 1.5.34 and earlier does not escape multiple fields inserted into the description of webhook-triggered builds, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.  |
| Git | 2.45.2 | CVE-2022-2257  | HIGH                 | 7.8        | Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.  |
| Git | 2.45.2 | CVE-2022-2279  | MEDIUM               | 5.5        | NULL Pointer Dereference in GitHub repository bfabiszewski/libmobi prior to 0.11.  |
| Git | 2.45.2 | CVE-2022-2280  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.19.  |
| Git | 2.45.2 | CVE-2022-2264  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.  |
| Git | 2.45.2 | CVE-2022-1983  | ['MEDIUM', 'MEDIUM'] | [6.5, 4.3] | Incorrect authorization in GitLab EE affecting all versions from 10.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allowed an attacker already in possession of a valid Deploy Key or a Deploy Token to misuse it from any location to access Container Registries even when IP address restrictions were configured. |
| Git | 2.45.2 | CVE-2022-2185  | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | A critical issue has been discovered in GitLab affecting all versions starting from 14.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 where an authenticated user authorized to import projects could import a maliciously crafted project leading to remote code execution.   |
| Git | 2.45.2 | CVE-2022-2227  | ['LOW', 'MEDIUM']    | [3.1, 4.3] | Improper access control in the runner jobs API in GitLab CE/EE affecting all versions prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows a previous maintainer of a project with a specific runner to access job and project meta data under certain conditions   |
| Git | 2.45.2 | CVE-2022-2230  | ['HIGH', 'MEDIUM']   | [8.1, 4.8] | A Stored Cross-Site Scripting vulnerability in the project settings page in GitLab CE/EE affecting all versions from 14.4 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf.  |
| Git | 2.45.2 | CVE-2022-2235  | ['HIGH', 'MEDIUM']   | [8.7, 5.4] | Insufficient sanitization in GitLab EE's external issue tracker affecting all versions from 14.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to perform cross-site scripting when a victim clicks on a maliciously crafted ZenTao link   |

|     |        |               |                      |            |   |
|-----|--------|---------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-2243 | ['MEDIUM', 'MEDIUM'] | [5.0, 4.3] | An access control vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows authenticated users to enumerate issues in non-linked sentry projects.  |
| Git | 2.45.2 | CVE-2022-2244 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An improper authorization vulnerability in GitLab EE/CE affecting all versions from 14.8 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows project members with reporter role to manage issues in project's error tracking feature.  |
| Git | 2.45.2 | CVE-2022-2250 | ['MEDIUM', 'MEDIUM'] | [4.7, 6.1] | An open redirect vulnerability in GitLab EE/CE affecting all versions from 11.1 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows an attacker to redirect users to an arbitrary location if they trust the URL.  |
| Git | 2.45.2 | CVE-2022-2281 | ['LOW', 'MEDIUM']    | [2.6, 5.3] | An information disclosure vulnerability in GitLab EE affecting all versions from 12.5 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1, allows disclosure of release titles if group milestones are associated with any project releases.   |
| Git | 2.45.2 | CVE-2022-1963 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab reveals if a user has enabled two-factor authentication on their account in the HTML source, to unauthenticated users.  |
| Git | 2.45.2 | CVE-2022-1981 | ['LOW', 'LOW']       | [2.7, 2.7] | An issue has been discovered in GitLab EE affecting all versions starting from 12.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. In GitLab, if a group enables the setting to restrict access to users belonging to specific domains, that allow-list may be bypassed if a Maintainer uses the 'Invite a group' feature to invite a group that has members that don't comply with domain allow-list. |
| Git | 2.45.2 | CVE-2022-1999 | ['LOW', 'MEDIUM']    | [3.1, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions from 8.13 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1. Under certain conditions, using the REST API an unprivileged user was able to change labels description.  |
| Git | 2.45.2 | CVE-2022-2228 | ['MEDIUM', 'MEDIUM'] | [5.3, 6.5] | Information exposure in GitLab EE affecting all versions from 12.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker with the appropriate access tokens to obtain CI variables in a group with using IP-based access restrictions even if the GitLab Runner is calling from outside the allowed IP range  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-2229  | ['HIGH', 'HIGH']     | [7.5, 7.5] | An improper authorization issue in GitLab CE/EE affecting all versions from 13.7 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to extract the value of an unprotected variable they know the name of in public projects or private projects they're a member of.  |
| Git | 2.45.2 | CVE-2022-2270  | ['LOW', 'MEDIUM']    | [3.5, 5.3] | An issue has been discovered in GitLab affecting all versions starting from 12.4 before 14.10.5, all versions starting from 15.0 before 15.0.4, all versions starting from 15.1 before 15.1.1. GitLab was leaking Conan packages names due to incorrect permissions verification.   |
| Git | 2.45.2 | CVE-2022-0167  | ['LOW', 'MEDIUM']    | [3.1, 6.1] | An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not disabling the Autocomplete attribute of fields related to sensitive information making it possible to be retrieved under certain conditions. |
| Git | 2.45.2 | CVE-2022-1954  | ['MEDIUM', 'MEDIUM'] | [4.3, 5.3] | A Regular Expression Denial of Service vulnerability in GitLab CE/EE affecting all versions from 1.0.2 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1 allows an attacker to make a GitLab instance inaccessible via specially crafted web server response headers   |
| Git | 2.45.2 | CVE-2022-25900 | ['HIGH', 'CRITICAL'] | [8.1, 9.8] | All versions of package git-clone are vulnerable to Command Injection due to insecure usage of the --upload-pack feature of git.  |
| Git | 2.45.2 | CVE-2022-2284  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2285  | HIGH                 | 7.8        | Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2286  | HIGH                 | 7.8        | Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2287  | HIGH                 | 7.1        | Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2290  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository zadam/trilium prior to 0.52.4, 0.53.1-beta.   |
| Git | 2.45.2 | CVE-2022-2288  | HIGH                 | 7.8        | Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.  |
| Git | 2.45.2 | CVE-2022-2289  | HIGH                 | 7.8        | Use After Free in GitHub repository vim/vim prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2300  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.19.   |
| Git | 2.45.2 | CVE-2022-2301  | MEDIUM               | 5.5        | Buffer Over-read in GitHub repository hpjansson/chafa prior to 1.10.3.  |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2022-2304  | HIGH     | 7.8 | Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.   |
| Git | 2.45.2 | CVE-2022-2321  | CRITICAL | 9.8 | Improper Restriction of Excessive Authentication Attempts in GitHub repository heroiclabs/nakama prior to 3.13.0. This results in login brute-force attacks.           |
| Git | 2.45.2 | CVE-2022-2342  | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository outline/outline prior to v0.64.4.   |
| Git | 2.45.2 | CVE-2022-2343  | HIGH     | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0044.   |
| Git | 2.45.2 | CVE-2022-2344  | HIGH     | 7.8 | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0045.   |
| Git | 2.45.2 | CVE-2022-2345  | HIGH     | 7.8 | Use After Free in GitHub repository vim/vim prior to 9.0.0046.   |
| Git | 2.45.2 | CVE-2022-2365  | MEDIUM   | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository zadam/trilium prior to 0.53.3.  |
| Git | 2.45.2 | CVE-2022-31501 | CRITICAL | 9.3 | The ChaoticOnyx/OnyxForum repository before 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                 |
| Git | 2.45.2 | CVE-2022-31502 | CRITICAL | 9.3 | The operatorequals/wormnest repository through 0.4.7 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                   |
| Git | 2.45.2 | CVE-2022-31503 | CRITICAL | 9.3 | The orchest/orchest repository before 2022.05.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                        |
| Git | 2.45.2 | CVE-2022-31504 | CRITICAL | 9.3 | The ChangeWeDer/BaiduWenkuSpider_flaskWeb repository before 2021-11-29 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31505 | CRITICAL | 9.3 | The cheo0/MercadoEnLineaBack repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.             |
| Git | 2.45.2 | CVE-2022-31506 | CRITICAL | 9.3 | The cmusatyalab/pendiamond repository through 10.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                   |
| Git | 2.45.2 | CVE-2022-31507 | CRITICAL | 9.3 | The ganga-devs/ganga repository before 8.5.10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                          |
| Git | 2.45.2 | CVE-2022-31508 | CRITICAL | 9.3 | The idayrus/evoting repository before 2022-05-08 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                       |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2022-31509 | CRITICAL | 9.3 | The iedaddata/usap-dc-website repository through 1.0.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                |
| Git | 2.45.2 | CVE-2022-31510 | CRITICAL | 9.3 | The sergeKashkin/Simple-RAT repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                              |
| Git | 2.45.2 | CVE-2022-31511 | CRITICAL | 9.3 | The AFDudley/equanimity repository through 2014-04-23 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                 |
| Git | 2.45.2 | CVE-2022-31512 | CRITICAL | 9.3 | The Atom02/flask-mvc repository through 2020-09-14 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                    |
| Git | 2.45.2 | CVE-2022-31513 | CRITICAL | 9.3 | The BolunHan/Krypton repository through 2021-06-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                    |
| Git | 2.45.2 | CVE-2022-31514 | CRITICAL | 9.3 | The Caoyongqi912/Fan_Platform repository through 2021-04-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                           |
| Git | 2.45.2 | CVE-2022-31515 | CRITICAL | 9.3 | The Delor4/CarceresBE repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.  |
| Git | 2.45.2 | CVE-2022-31516 | CRITICAL | 9.3 | The Harveyzyh/Python repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                    |
| Git | 2.45.2 | CVE-2022-31517 | CRITICAL | 9.3 | The HolgerGraef/MSM repository through 2021-04-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                     |
| Git | 2.45.2 | CVE-2022-31518 | CRITICAL | 9.3 | The JustAnotherSoftwareDeveloper/Python-Recipe-Database repository through 2021-03-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31519 | CRITICAL | 9.3 | The Lukasavicus/WindMill repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                       |
| Git | 2.45.2 | CVE-2022-31520 | CRITICAL | 9.3 | The Luxas98/logstash-management-api repository through 2020-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                     |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2022-31521 | CRITICAL | 9.3 | The Niyaz-Mohamed/mosaic repository through 1.0.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                        |
| Git | 2.45.2 | CVE-2022-31522 | CRITICAL | 9.3 | The NotVinay/karaokey repository through 2019-12-11 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                      |
| Git | 2.45.2 | CVE-2022-31523 | CRITICAL | 9.3 | The PaddlePaddle/Anakin repository through 0.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                         |
| Git | 2.45.2 | CVE-2022-31524 | CRITICAL | 9.3 | The PureStorage-OpenConnect/swagger repository through 1.1.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.             |
| Git | 2.45.2 | CVE-2022-31525 | CRITICAL | 9.3 | The SummaLabs/DLS repository through 0.1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                               |
| Git | 2.45.2 | CVE-2022-31526 | CRITICAL | 9.3 | The ThundeRatz/ThunderDocs repository through 2020-05-01 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                 |
| Git | 2.45.2 | CVE-2022-31527 | CRITICAL | 9.3 | The Wildog/flask-file-server repository through 2020-02-20 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.               |
| Git | 2.45.2 | CVE-2022-31528 | CRITICAL | 9.3 | The bonn-activity-maps/bam_annotation_tool repository through 2021-08-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31529 | CRITICAL | 9.3 | The cinemaproject/monorepo repository through 2021-03-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                 |
| Git | 2.45.2 | CVE-2022-31530 | CRITICAL | 9.3 | The csm-aut/csm repository through 3.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                                   |
| Git | 2.45.2 | CVE-2022-31531 | CRITICAL | 9.3 | The daunst/cilantro repository through 0.0.4 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                             |
| Git | 2.45.2 | CVE-2022-31532 | CRITICAL | 9.3 | The dankolbman/travel_blahg repository through 2016-01-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                |

|     |        |                |          |     |   |
|-----|--------|----------------|----------|-----|---|
| Git | 2.45.2 | CVE-2022-31533 | CRITICAL | 9.3 | The decentraminds/umbral repository through 2020-01-15 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.              |
| Git | 2.45.2 | CVE-2022-31534 | CRITICAL | 9.3 | The echoleegroup/PythonWeb repository through 2018-10-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.            |
| Git | 2.45.2 | CVE-2022-31535 | CRITICAL | 9.3 | The freefood89/Fishtank repository through 2015-06-24 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.               |
| Git | 2.45.2 | CVE-2022-31536 | CRITICAL | 9.3 | The jaygarza1982/ytdl-sync repository through 2021-01-02 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.            |
| Git | 2.45.2 | CVE-2022-31537 | CRITICAL | 9.3 | The jmcginty15/Solar-system-simulator repository through 2021-07-26 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31538 | CRITICAL | 9.3 | The joaopedro-fg/mp-m08-interface repository through 2020-12-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.     |
| Git | 2.45.2 | CVE-2022-31539 | CRITICAL | 9.3 | The kotekan/kotekan repository through 2021.11 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                      |
| Git | 2.45.2 | CVE-2022-31540 | CRITICAL | 9.3 | The kumardeepak/hin-eng-preprocessing repository through 2019-07-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31541 | CRITICAL | 9.3 | The lyubolp/Barry-Voice-Assistant repository through 2021-01-18 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.     |
| Git | 2.45.2 | CVE-2022-31542 | CRITICAL | 9.3 | The mandoku/mdweb repository through 2015-05-07 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                     |
| Git | 2.45.2 | CVE-2022-31543 | CRITICAL | 9.3 | The maxtortime/SetupBox repository through 1.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                      |
| Git | 2.45.2 | CVE-2022-31544 | CRITICAL | 9.3 | The meerstein/rbtl repository through 1.5 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                           |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2022-31545 | CRITICAL | 9.3 | The ml-inory/ModelConverter repository through 2021-04-26 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                    |
| Git | 2.45.2 | CVE-2022-31546 | CRITICAL | 9.3 | The nlpweb/glance repository through 2014-06-27 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                              |
| Git | 2.45.2 | CVE-2022-31547 | CRITICAL | 9.3 | The noamezekiel/sphere repository through 2020-05-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                         |
| Git | 2.45.2 | CVE-2022-31548 | CRITICAL | 9.3 | The nrlakin/homepage repository through 2017-03-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                           |
| Git | 2.45.2 | CVE-2022-31549 | CRITICAL | 9.3 | The olmax99/helm-flask-celery repository before 2022-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                   |
| Git | 2.45.2 | CVE-2022-31550 | CRITICAL | 9.3 | The olmax99/pyathenastack repository through 2019-11-08 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                      |
| Git | 2.45.2 | CVE-2022-31551 | CRITICAL | 9.3 | The pleomax00/flask-mongo-skel repository through 2012-11-01 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                 |
| Git | 2.45.2 | CVE-2022-31552 | CRITICAL | 9.3 | The project-anuvaad/anuvaad-corpus repository through 2020-11-23 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.             |
| Git | 2.45.2 | CVE-2022-31553 | CRITICAL | 9.3 | The rainsoupah/sleep-learner repository through 2021-02-21 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                   |
| Git | 2.45.2 | CVE-2022-31554 | CRITICAL | 9.3 | The rohitnayak/movie-review-sentiment-analysis repository through 2017-05-07 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31555 | CRITICAL | 9.3 | The romain20100/nursequest repository through 2018-02-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                     |
| Git | 2.45.2 | CVE-2022-31556 | CRITICAL | 9.3 | The rusyasoft/TrainEnergyServer repository through 2017-08-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2022-31557 | CRITICAL | 9.3 | The seveas/golem repository through 2016-05-17 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                     |
| Git | 2.45.2 | CVE-2022-31558 | CRITICAL | 9.3 | The tooxie/shiva-server repository through 0.10.0 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                  |
| Git | 2.45.2 | CVE-2022-31559 | CRITICAL | 9.3 | The tsileo/flask-yeoman repository through 2013-09-13 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.              |
| Git | 2.45.2 | CVE-2022-31560 | CRITICAL | 9.3 | The uncleYiba/photo_tag repository through 2020-08-31 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.              |
| Git | 2.45.2 | CVE-2022-31561 | CRITICAL | 9.3 | The varijkapil13/Sphere_ImageBackend repository through 2019-10-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31562 | CRITICAL | 9.3 | The waveyan/internshipsystem repository through 2018-05-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.         |
| Git | 2.45.2 | CVE-2022-31563 | CRITICAL | 9.3 | The whmacmac/vprj repository through 2022-04-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                    |
| Git | 2.45.2 | CVE-2022-31564 | CRITICAL | 9.3 | The woduq1414/munhak-moa repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.              |
| Git | 2.45.2 | CVE-2022-31565 | CRITICAL | 9.3 | The yogson/syrabond repository through 2020-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                  |
| Git | 2.45.2 | CVE-2022-31566 | HIGH     | 8.6 | The DSAB-local/DSAB repository through 2019-02-18 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                  |
| Git | 2.45.2 | CVE-2022-31567 | CRITICAL | 9.3 | The DSABenchmark/DSAB repository through 2.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                       |
| Git | 2.45.2 | CVE-2022-31568 | CRITICAL | 9.3 | The Rexians/rex-web repository through 2022-06-05 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                  |

|     |        |                |          |     |  |
|-----|--------|----------------|----------|-----|--|
| Git | 2.45.2 | CVE-2022-31570 | CRITICAL | 9.8 | The adriankoczuruek/ceneo-web-scraper repository through 2021-03-15 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.    |
| Git | 2.45.2 | CVE-2022-31571 | CRITICAL | 9.3 | The akashtalole/python-flask-restful-api repository through 2019-09-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31572 | CRITICAL | 9.3 | The ceee-vip/cockybook repository through 2015-04-16 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                   |
| Git | 2.45.2 | CVE-2022-31573 | CRITICAL | 9.3 | The chainer/chainerml-visualizer repository through 0.1.1 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.              |
| Git | 2.45.2 | CVE-2022-31574 | CRITICAL | 9.3 | The deepaliupadhyay/RealEstate repository through 2018-11-30 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.           |
| Git | 2.45.2 | CVE-2022-31575 | CRITICAL | 9.3 | The duducosmos/livro_python repository through 2018-06-06 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.              |
| Git | 2.45.2 | CVE-2022-31576 | CRITICAL | 9.3 | The heidi-luong1109/shackerpanel repository through 2021-05-25 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.         |
| Git | 2.45.2 | CVE-2022-31577 | CRITICAL | 9.3 | The longmaoteamtf/audio_aligner_app repository through 2020-01-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.      |
| Git | 2.45.2 | CVE-2022-31578 | HIGH     | 7.5 | The piaoyunsoft/bt_Inmp repository through 2019-10-10 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                  |
| Git | 2.45.2 | CVE-2022-31579 | CRITICAL | 9.3 | The ralphjzhang/iasset repository through 2022-05-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                   |
| Git | 2.45.2 | CVE-2022-31580 | CRITICAL | 9.3 | The sanojtharindu/caretakerr-api repository through 2021-05-17 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.         |
| Git | 2.45.2 | CVE-2022-31581 | CRITICAL | 9.3 | The scorelab/OpenMF repository before 2022-05-03 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                       |

|     |        |                |                        |            |   |
|-----|--------|----------------|------------------------|------------|---|
| Git | 2.45.2 | CVE-2022-31582 | CRITICAL               | 9.3        | The shaolo1/VideoServer repository through 2019-09-21 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                 |
| Git | 2.45.2 | CVE-2022-31583 | CRITICAL               | 9.3        | The sravaniboinepelli/AutomatedQuizEval repository through 2020-04-27 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31584 | CRITICAL               | 9.3        | The stonethree/s3label repository through 2019-08-14 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                  |
| Git | 2.45.2 | CVE-2022-31585 | CRITICAL               | 9.3        | The umeshpatil-dev/Home__internet repository through 2020-08-28 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.       |
| Git | 2.45.2 | CVE-2022-31586 | CRITICAL               | 9.3        | The unizar-30226-2019-06/ChangePop-Back repository through 2019-06-04 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely. |
| Git | 2.45.2 | CVE-2022-31587 | CRITICAL               | 9.3        | The yuriyouzhou/KG-fashion-chatbot repository through 2018-05-22 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.      |
| Git | 2.45.2 | CVE-2022-31588 | CRITICAL               | 9.3        | The zippies/testplatform repository through 2016-07-19 on GitHub allows absolute path traversal because the Flask send_file function is used unsafely.                |
| Git | 2.45.2 | CVE-2022-2368  | ['MEDIUM', 'CRITICAL'] | [6.5, 9.8] | Authentication Bypass by Spoofing in GitHub repository microweber/microweber prior to 1.2.20.   |

|     |        |                |                   |            |  |
|-----|--------|----------------|-------------------|------------|--|
| Git | 2.45.2 | CVE-2022-29187 | ['HIGH', 'HIGH']  | [7.8, 7.8] | Git is a distributed revision control system. Git prior to versions 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4, and 2.30.5, is vulnerable to privilege escalation in all platforms. An unsuspecting user could still be affected by the issue reported in CVE-2022-24765, for example when navigating as root into a shared tmp directory that is owned by them, but where an attacker could create a git repository. Versions 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4, and 2.30.5 contain a patch for this issue. The simplest way to avoid being affected by the exploit described in the example is to avoid running git as root (or an Administrator in Windows), and if needed to reduce its use to a minimum. While a generic workaround is not possible, a system could be hardened from the exploit described in the example by removing any such repository if it exists already and creating one as root to block any future attacks.   |
| Git | 2.45.2 | CVE-2022-31012 | ['HIGH', 'HIGH']  | [8.2, 7.3] | Git for Windows is a fork of Git that contains Windows-specific patches. This vulnerability in versions prior to 2.37.1 lets Git for Windows' installer execute a binary into `C:\mingw64\bin\git.exe` by mistake. This only happens upon a fresh install, not when upgrading Git for Windows. A patch is included in version 2.37.1. Two workarounds are available. Create the `C:\mingw64` folder and remove read/write access from this folder, or disallow arbitrary authenticated users to create folders in `C:\`.   |
| Git | 2.45.2 | CVE-2022-31102 | ['LOW', 'MEDIUM'] | [2.6, 6.1] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with 2.3.0 and prior to 2.3.6 and 2.4.5 is vulnerable to a cross-site scripting (XSS) bug which could allow an attacker to inject arbitrary JavaScript in the `/auth/callback` page in a victim's browser. This vulnerability only affects Argo CD instances which have single sign on (SSO) enabled. The exploit also assumes the attacker has 1) access to the API server's encryption key, 2) a method to add a cookie to the victim's browser, and 3) the ability to convince the victim to visit a malicious `/auth/callback` link. The vulnerability is classified as low severity because access to the API server's encryption key already grants a high level of access. Exploiting the XSS would allow the attacker to impersonate the victim, but would not grant any privileges which the attacker could not otherwise gain using the encryption key. A patch for this vulnerability has been released in the following Argo C... |

|     |        |                |                      |            |  |
|-----|--------|----------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-31105 | ['HIGH', 'CRITICAL'] | [8.3, 9.6] | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 0.4.0 and prior to 2.2.11, 2.3.6, and 2.4.5 is vulnerable to an improper certificate validation bug which could cause Argo CD to trust a malicious (or otherwise untrustworthy) OpenID Connect (OIDC) provider. A patch for this vulnerability has been released in Argo CD versions 2.4.5, 2.3.6, and 2.2.11. There are no complete workarounds, but a partial workaround is available. Those who use an external OIDC provider (not the bundled Dex instance), can mitigate the issue by setting the `oidc.config.rootCA` field in the `argocd-cm` ConfigMap. This mitigation only forces certificate validation when the API server handles login flows. It does not force certificate verification when verifying tokens on API calls. |
| Git | 2.45.2 | CVE-2022-25891 | ['HIGH', 'HIGH']     | [7.5, 7.5] | The package github.com/containrrr/shoutrr/pkg/util before 0.6.0 are vulnerable to Denial of Service (DoS) via the util.PartitionMessage function. Exploiting this vulnerability is possible by sending exactly 2000, 4000, or 6000 characters messages.  |
| Git | 2.45.2 | CVE-2022-2400  | MEDIUM               | 5.3        | External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.   |
| Git | 2.45.2 | CVE-2022-2453  | HIGH                 | 7.8        | Use After Free in GitHub repository gpac/gpac prior to 2.1-DEV.  |
| Git | 2.45.2 | CVE-2022-2454  | HIGH                 | 7.8        | Integer Overflow or Wraparound in GitHub repository gpac/gpac prior to 2.1-DEV.  |
| Git | 2.45.2 | CVE-2022-2493  | HIGH                 | 8.1        | Data Access from Outside Expected Data Manager Component in GitHub repository openemr/openemr prior to 7.0.0.  |
| Git | 2.45.2 | CVE-2022-2494  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.0.   |
| Git | 2.45.2 | CVE-2022-2495  | MEDIUM               | 4.8        | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.21.  |
| Git | 2.45.2 | CVE-2022-2470  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.21.   |
| Git | 2.45.2 | CVE-2020-28422 | ['MEDIUM', 'HIGH']   | [6.4, 7.8] | All versions of package git-archive are vulnerable to Command Injection via the exports function.  |
| Git | 2.45.2 | CVE-2022-2522  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0061.   |
| Git | 2.45.2 | CVE-2022-2523  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository beancount/fava prior to 1.22.2.  |
| Git | 2.45.2 | CVE-2022-2549  | MEDIUM               | 5.5        | NULL Pointer Dereference in GitHub repository gpac/gpac prior to v2.1.0-DEV.   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-2550  | HIGH               | 8.8        | OS Command Injection in GitHub repository hestiacp/hestiacp prior to 1.6.5.   |
| Git | 2.45.2 | CVE-2022-36881 | HIGH               | 8.1        | Jenkins Git client Plugin 3.11.0 and earlier does not perform SSH host key verification when connecting to Git repositories via SSH, enabling man-in-the-middle attacks.  |
| Git | 2.45.2 | CVE-2022-36882 | HIGH               | 8.8        | A cross-site request forgery (CSRF) vulnerability in Jenkins Git Plugin 4.11.3 and earlier allows attackers to trigger builds of jobs configured to use an attacker-specified Git repository and to cause them to check out an attacker-specified commit.   |
| Git | 2.45.2 | CVE-2022-36883 | HIGH               | 7.5        | A missing permission check in Jenkins Git Plugin 4.11.3 and earlier allows unauthenticated attackers to trigger builds of jobs configured to use an attacker-specified Git repository and to cause them to check out an attacker-specified commit.  |
| Git | 2.45.2 | CVE-2022-36884 | MEDIUM             | 5.3        | The webhook endpoint in Jenkins Git Plugin 4.11.3 and earlier provide unauthenticated attackers information about the existence of jobs configured to use an attacker-specified Git repository.   |
| Git | 2.45.2 | CVE-2022-36885 | MEDIUM             | 5.3        | Jenkins GitHub Plugin 1.34.4 and earlier uses a non-constant time comparison function when checking whether the provided and computed webhook signatures are equal, allowing attackers to use statistical methods to obtain a valid webhook signature.  |
| Git | 2.45.2 | CVE-2022-1948  | ['HIGH', 'MEDIUM'] | [8.7, 5.4] | An issue has been discovered in GitLab affecting all versions starting from 15.0 before 15.0.1. Missing validation of input used in quick actions allowed an attacker to exploit XSS by injecting HTML in contact details.  |
| Git | 2.45.2 | CVE-2022-2564  | CRITICAL           | 9.8        | Prototype Pollution in GitHub repository automattic/mongoose prior to 6.4.6.  |
| Git | 2.45.2 | CVE-2022-24912 | ['HIGH', 'HIGH']   | [7.5, 7.5] | The package github.com/runatlantis/atlantis/server/controllers/events before 0.19.7 are vulnerable to Timing Attack in the webhook event validator code, which does not use a constant-time comparison function to validate the webhook secret. It can allow an attacker to recover this secret as an attacker and then forge webhook events. |
| Git | 2.45.2 | CVE-2022-2571  | HIGH               | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0101.  |
| Git | 2.45.2 | CVE-2022-2580  | HIGH               | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0102.  |
| Git | 2.45.2 | CVE-2022-2581  | HIGH               | 7.8        | Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.0104.  |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2022-2589  | MEDIUM                   | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository beancount/fava prior to 1.22.3.  |
| Git | 2.45.2 | CVE-2022-2595  | CRITICAL                 | 10.0       | Improper Authorization in GitHub repository kromitgmbh/titra prior to 0.79.1.  |
| Git | 2.45.2 | CVE-2022-2596  | ['MEDIUM', 'MEDIUM']     | [5.9, 5.9] | Inefficient Regular Expression Complexity in GitHub repository node-fetch/node-fetch prior to 3.2.10.  |
| Git | 2.45.2 | CVE-2022-2598  | ['MEDIUM', 'MEDIUM']     | [6.5, 5.5] | Out-of-bounds Write to API in GitHub repository vim/vim prior to 9.0.0100.   |
| Git | 2.45.2 | CVE-2022-31128 | ['MEDIUM', 'MEDIUM']     | [5.4, 5.4] | Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions Tuleap does not properly verify permissions when creating branches with the REST API in Git repositories using the fine grained permissions. Users can create branches via the REST endpoint `POST git/:id/branches` regardless of the permissions set on the repository. This issue has been fixed in version 13.10.99.82 Tuleap Community Edition as well as in version 13.10-3 of Tuleap Enterprise Edition. Users are advised to upgrade. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2020-28434 | ['CRITICAL', 'CRITICAL'] | [9.4, 9.8] | This affects all versions of package gitblame. The injection point is located in line 15 in lib/gitblame.js.   |
| Git | 2.45.2 | CVE-2022-23733 | MEDIUM                   | 5.4        | A stored XSS vulnerability was identified in GitHub Enterprise Server that allowed the injection of arbitrary attributes. This injection was blocked by Github's Content Security Policy (CSP). This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.3.11, 3.4.6 and 3.5.3. This vulnerability was reported via the GitHub Bug Bounty program.  |
| Git | 2.45.2 | CVE-2022-2631  | HIGH                     | 8.8        | Improper Access Control in GitHub repository tooljet/tooljet prior to v1.19.0.   |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35928 | ['HIGH', 'MEDIUM']   | [8.4, 5.5] | AES Crypt is a file encryption software for multiple platforms. AES Crypt for Linux built using the source on GitHub and having the version number 3.11 has a vulnerability with respect to reading user-provided passwords and confirmations via command-line prompts. Passwords lengths were not checked before being read. This vulnerability may lead to buffer overruns. This does <u>not</u> affect source code found on aescrypt.com, nor is the vulnerability present when providing a password or a key via the <code>`-p`</code> or <code>`-k`</code> command-line options. The problem was fixed via in commit 68761851b and will be included in release 3.16. Users are advised to upgrade. Users unable to upgrade should use the <code>`-p`</code> or <code>`-k`</code> options to provide a password or key. |
| Git | 2.45.2 | CVE-2022-2651  | CRITICAL             | 9.8        | Authentication Bypass by Primary Weakness in GitHub repository bookwyrms-social/bookwyrms prior to 0.4.5.   |
| Git | 2.45.2 | CVE-2022-2626  | HIGH                 | 7.2        | Incorrect Privilege Assignment in GitHub repository hestiacp/hestiacp prior to 1.6.6.   |
| Git | 2.45.2 | CVE-2022-2636  | ['HIGH', 'HIGH']     | [8.5, 8.8] | Improper Control of Generation of Code ('Code Injection') in GitHub repository hestiacp/hestiacp prior to 1.6.6.  |
| Git | 2.45.2 | CVE-2022-2095  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An improper access control check in GitLab CE/EE affecting all versions starting from 13.7 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious authenticated user to view a public project's Deploy Key's public fingerprint and name when that key has write permission. Note that GitLab never asks for nor stores the private key.  |
| Git | 2.45.2 | CVE-2022-2303  | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for group members to bypass 2FA enforcement enabled at the group level by using Resource Owner Password Credentials grant to obtain an access token without using 2FA.  |
| Git | 2.45.2 | CVE-2022-2307  | ['LOW', 'LOW']       | [3.5, 3.8] | A lack of cascading deletes in GitLab CE/EE affecting all versions starting from 13.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious Group Owner to retain a usable Group Access Token even after the Group is deleted, though the APIs usable by that token are limited.   |

|     |        |               |                      |            |  |
|-----|--------|---------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-2326 | ['MEDIUM', 'HIGH']   | [6.4, 8.1] | An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible to gain access to a private project through an email invite by using other user's email address as an unverified secondary email.  |
| Git | 2.45.2 | CVE-2022-2417 | ['MEDIUM', 'MEDIUM'] | [6.2, 4.5] | Insufficient validation in GitLab CE/EE affecting all versions from 12.10 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an authenticated and authorised user to import a project that includes branch names which are 40 hexadecimal characters, which could be abused in supply chain attacks where a victim pinned to a specific Git commit of the project.                             |
| Git | 2.45.2 | CVE-2022-2456 | ['MEDIUM', 'LOW']    | [4.9, 2.7] | An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for malicious group or project maintainers to change their corresponding group or project visibility by crafting a malicious POST request.   |
| Git | 2.45.2 | CVE-2022-2459 | ['LOW', 'LOW']       | [2.7, 2.7] | An issue has been discovered in GitLab EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for email invited members to join a project even after the Group Owner has enabled the setting to prevent members from being added to projects in a group, if the invite was sent before the setting was enabled. |
| Git | 2.45.2 | CVE-2022-2497 | ['HIGH', 'MEDIUM']   | [8.5, 6.4] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. A malicious developer could exfiltrate an integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server.                              |
| Git | 2.45.2 | CVE-2022-2498 | ['MEDIUM', 'HIGH']   | [6.4, 7.5] | An issue in pipeline subscriptions in GitLab EE affecting all versions from 12.8 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 triggered new pipelines with the person who created the tag as the pipeline creator instead of the subscription's author.   |

|     |        |               |                      |            |  |
|-----|--------|---------------|----------------------|------------|--|
| Git | 2.45.2 | CVE-2022-2499 | ['LOW', 'MEDIUM']    | [3.5, 4.3] | An issue has been discovered in GitLab EE affecting all versions starting from 13.10 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab's Jira integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Jira issues.  |
| Git | 2.45.2 | CVE-2022-2500 | ['MEDIUM', 'MEDIUM'] | [4.4, 5.4] | A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1. A stored XSS flaw in job error messages allows attackers to perform arbitrary actions on behalf of victims at client side.  |
| Git | 2.45.2 | CVE-2022-2501 | ['MEDIUM', 'HIGH']   | [5.9, 7.5] | An improper access control issue in GitLab EE affecting all versions from 12.0 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an attacker to bypass IP allow-listing and download artifacts. This attack only bypasses IP allow-listing, proper permissions are still required.  |
| Git | 2.45.2 | CVE-2022-2512 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. Membership changes are not reflected in TODO for confidential notes, allowing a former project members to read updates via TODOs.  |
| Git | 2.45.2 | CVE-2022-2531 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab EE affecting all versions starting from 12.5 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was not performing correct authentication on Grafana API under specific conditions allowing unauthenticated users to perform queries through a path traversal vulnerability. |
| Git | 2.45.2 | CVE-2022-2534 | ['LOW', 'MEDIUM']    | [2.2, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was returning contributor emails due to improper data handling in the Datadog integration.   |
| Git | 2.45.2 | CVE-2022-2539 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.6 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1, allowed a project member to filter issues by contact and organization.   |
| Git | 2.45.2 | CVE-2022-2713 | CRITICAL             | 9.8        | Insufficient Session Expiration in GitHub repository cockpit-hq/cockpit prior to 2.2.0.  |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-2729  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - DOM in GitHub repository openemr/openemr prior to 7.0.0.1.   |
| Git | 2.45.2 | CVE-2022-2730  | MEDIUM               | 6.5        | Authorization Bypass Through User-Controlled Key in GitHub repository openemr/openemr prior to 7.0.0.1.   |
| Git | 2.45.2 | CVE-2022-2731  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1.   |
| Git | 2.45.2 | CVE-2022-2732  | ['HIGH', 'HIGH']     | [8.3, 8.3] | Missing Authorization in GitHub repository openemr/openemr prior to 7.0.0.1.  |
| Git | 2.45.2 | CVE-2022-2733  | MEDIUM               | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1.   |
| Git | 2.45.2 | CVE-2022-2734  | MEDIUM               | 5.4        | Improper Restriction of Rendered UI Layers or Frames in GitHub repository openemr/openemr prior to 7.0.0.1.   |
| Git | 2.45.2 | CVE-2022-2756  | MEDIUM               | 6.5        | Server-Side Request Forgery (SSRF) in GitHub repository kareadita/kavita prior to 0.5.4.1.  |
| Git | 2.45.2 | CVE-2022-2777  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.1.  |
| Git | 2.45.2 | CVE-2022-38183 | MEDIUM               | 6.5        | In Gitea before 1.16.9, it was possible for users to add existing issues to projects. Due to improper access controls, an attacker could assign any issue to any project in Gitea (there was no permission check for fetching the issue). As a result, the attacker would get access to private issue titles. |
| Git | 2.45.2 | CVE-2022-2818  | ['CRITICAL', 'HIGH'] | [9.8, 8.8] | Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository cockpit-hq/cockpit prior to 2.2.2.  |
| Git | 2.45.2 | CVE-2022-2819  | HIGH                 | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0211.  |
| Git | 2.45.2 | CVE-2022-2820  | ['HIGH', 'HIGH']     | [7.0, 8.2] | Session Fixation in GitHub repository namelessmc/nameless prior to v2.0.2.  |
| Git | 2.45.2 | CVE-2022-2821  | HIGH                 | 7.5        | Missing Critical Step in Authentication in GitHub repository namelessmc/nameless prior to v2.0.2.   |

|     |        |                |                          |            |   |
|-----|--------|----------------|--------------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35954 | ['MEDIUM', 'MEDIUM']     | [5.0, 5.0] | The GitHub Actions ToolKit provides a set of packages to make creating actions easier. The <code>`core.exportVariable`</code> function uses a well known delimiter that attackers can use to break out of that specific variable and assign values to other arbitrary variables. Workflows that write untrusted values to the <code>`GITHUB_ENV`</code> file may cause the path or other environment variables to be modified without the intention of the workflow or action author. Users should upgrade to <code>`@actions/core v1.9.1`</code> . If you are unable to upgrade the <code>`@actions/core`</code> package, you can modify your action to ensure that any user input does not contain the delimiter <code>`_GitHubActionsFileCommandDelimiter_`</code> before calling <code>`core.exportVariable`</code> . |
| Git | 2.45.2 | CVE-2022-2824  | ['HIGH', 'MEDIUM']       | [8.8, 5.4] | Authorization Bypass Through User-Controlled Key in GitHub repository openemr/openemr prior to 7.0.0.1.   |
| Git | 2.45.2 | CVE-2022-2816  | HIGH                     | 7.8        | Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.0212.  |
| Git | 2.45.2 | CVE-2022-2817  | HIGH                     | 7.8        | Use After Free in GitHub repository vim/vim prior to 9.0.0213.  |
| Git | 2.45.2 | CVE-2022-2871  | MEDIUM                   | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository notrnos/notrnoserp prior to 0.7.   |
| Git | 2.45.2 | CVE-2022-2845  | ['HIGH', 'HIGH']         | [7.8, 7.8] | Improper Validation of Specified Quantity in Input in GitHub repository vim/vim prior to 9.0.0218.  |
| Git | 2.45.2 | CVE-2022-2849  | HIGH                     | 7.8        | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0220.  |
| Git | 2.45.2 | CVE-2022-2862  | HIGH                     | 7.8        | Use After Free in GitHub repository vim/vim prior to 9.0.0221.  |
| Git | 2.45.2 | CVE-2022-2874  | MEDIUM                   | 5.5        | NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0224.  |
| Git | 2.45.2 | CVE-2022-35975 | ['CRITICAL', 'CRITICAL'] | [9.0, 9.8] | The GitOps Tools Extension for VSCode can make it easier to manage Flux objects. A specially crafted Flux object may allow for remote code execution in the machine running the extension, in the context of the user that is running VSCode. Users using the VSCode extension to manage clusters that are shared amongst other users are affected by this issue. The only safe mitigation is to update to the latest version of the extension.   |

|     |        |                |                        |            |  |
|-----|--------|----------------|------------------------|------------|--|
| Git | 2.45.2 | CVE-2021-32862 | ['HIGH', 'MEDIUM']     | [7.5, 5.4] | The GitHub Security Lab discovered sixteen ways to exploit a cross-site scripting vulnerability in nbconvert. When using nbconvert to generate an HTML version of a user-controllable notebook, it is possible to inject arbitrary HTML which may lead to cross-site scripting (XSS) vulnerabilities if these HTML notebooks are served by a web server (eg: nbviewer).  |
| Git | 2.45.2 | CVE-2022-35976 | ['MEDIUM', 'CRITICAL'] | [5.2, 9.8] | The GitOps Tools Extension for VSCode relies on kubeconfigs in order to communicate with Kubernetes clusters. A specially crafted kubeconfig leads to arbitrary code execution on behalf of the user running VSCode. Users relying on kubeconfigs that are generated or altered by other processes or users are affected by this issue. Please note that the vulnerability is specific to this extension, and the same kubeconfig would not result in arbitrary code execution when used with kubectl. Using only trust-worthy kubeconfigs is a safe mitigation. However, updating to the latest version of the extension is still highly recommended. |
| Git | 2.45.2 | CVE-2022-1021  | MEDIUM                 | 5.4        | Insecure Storage of Sensitive Information in GitHub repository chatwoot/chatwoot prior to 2.6.0.   |
| Git | 2.45.2 | CVE-2022-2889  | HIGH                   | 7.8        | Use After Free in GitHub repository vim/vim prior to 9.0.0225.   |
| Git | 2.45.2 | CVE-2022-0542  | MEDIUM                 | 6.1        | Cross-site Scripting (XSS) - DOM in GitHub repository chatwoot/chatwoot prior to 2.7.0.  |
| Git | 2.45.2 | CVE-2022-2921  | HIGH                   | 8.8        | Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository notrinos/notrinoserp prior to v0.7. This results in privilege escalation to a system administrator account. An attacker can gain access to protected functionality such as create/update companies, install/update languages, install/activate extensions, install/activate themes and other permissive actions.  |
| Git | 2.45.2 | CVE-2022-2885  | MEDIUM                 | 4.8        | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.   |
| Git | 2.45.2 | CVE-2022-2927  | CRITICAL               | 9.8        | Weak Password Requirements in GitHub repository notrinos/notrinoserp prior to 0.7.   |
| Git | 2.45.2 | CVE-2022-1340  | MEDIUM                 | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.   |
| Git | 2.45.2 | CVE-2022-2930  | HIGH                   | 7.8        | Unverified Password Change in GitHub repository octoprint/octoprint prior to 1.8.3.  |

|     |        |                |        |     |   |
|-----|--------|----------------|--------|-----|---|
| Git | 2.45.2 | CVE-2022-2890  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.  |
| Git | 2.45.2 | CVE-2022-2932  | MEDIUM | 6.1 | Cross-site Scripting (XSS) - Reflected in GitHub repository bustle/mobiledoc-kit prior to 0.14.2.   |
| Git | 2.45.2 | CVE-2022-2923  | MEDIUM | 5.5 | NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0240.  |
| Git | 2.45.2 | CVE-2022-2829  | MEDIUM | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.  |
| Git | 2.45.2 | CVE-2022-2796  | MEDIUM | 4.8 | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.4.   |
| Git | 2.45.2 | CVE-2022-2965  | MEDIUM | 4.3 | Improper Restriction of Rendered UI Layers or Frames in GitHub repository notrinos/notrinosep prior to 0.7.   |
| Git | 2.45.2 | CVE-2022-2946  | HIGH   | 7.8 | Use After Free in GitHub repository vim/vim prior to 9.0.0246.  |
| Git | 2.45.2 | CVE-2022-38663 | MEDIUM | 6.5 | Jenkins Git Plugin 4.11.4 and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log provided by the Git Username and Password (`gitUsernamePassword`) credentials binding. |
| Git | 2.45.2 | CVE-2022-2980  | MEDIUM | 5.5 | NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0259.  |
| Git | 2.45.2 | CVE-2022-2982  | HIGH   | 7.8 | Use After Free in GitHub repository vim/vim prior to 9.0.0260.  |
| Git | 2.45.2 | CVE-2022-2997  | HIGH   | 8.0 | Session Fixation in GitHub repository snipe/snipe-it prior to 6.0.10.   |
| Git | 2.45.2 | CVE-2022-3016  | HIGH   | 7.8 | Use After Free in GitHub repository vim/vim prior to 9.0.0286.  |
| Git | 2.45.2 | CVE-2022-3017  | MEDIUM | 6.5 | Cross-Site Request Forgery (CSRF) in GitHub repository froxlor/froxlor prior to 0.10.38.  |
| Git | 2.45.2 | CVE-2022-3035  | MEDIUM | 4.8 | Cross-site Scripting (XSS) - Stored in GitHub repository snipe/snipe-it prior to v6.0.11.   |
| Git | 2.45.2 | CVE-2022-3037  | HIGH   | 7.8 | Use After Free in GitHub repository vim/vim prior to 9.0.0322.  |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2022-36035 | ['HIGH', 'HIGH'] | [7.7, 7.8] | Flux is a tool for keeping Kubernetes clusters in sync with sources of configuration (like Git repositories), and automating updates to configuration when there is new code to deploy. Flux CLI allows users to deploy Flux components into a Kubernetes cluster via command-line. The vulnerability allows other applications to replace the Flux deployment information with arbitrary content which is deployed into the target Kubernetes cluster instead. The vulnerability is due to the improper handling of user-supplied input, which results in a path traversal that can be controlled by the attacker. Users sharing the same shell between other applications and the Flux CLI commands could be affected by this vulnerability. In some scenarios no errors may be presented, which may cause end users not to realize that something is amiss. A safe workaround is to execute Flux CLI in ephemeral and isolated shell environments, which can ensure no persistent values exist from previous processes. However, u... |
| Git | 2.45.2 | CVE-2022-3072  | MEDIUM           | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 8.9.3.  |
| Git | 2.45.2 | CVE-2022-38790 | MEDIUM           | 5.4        | Weave GitOps Enterprise before 0.9.0-rc.5 has a cross-site scripting (XSS) bug allowing a malicious user to inject a javascript: link in the UI. When clicked by a victim user, the script will execute with the victim's permission. The exposure appears in Weave GitOps Enterprise UI via a GitopsCluster dashboard link. An annotation can be added to a GitopsCluster custom resource.  |
| Git | 2.45.2 | CVE-2022-3065  | HIGH             | 7.5        | Improper Access Control in GitHub repository jgraph/drawio prior to 20.2.8.  |
| Git | 2.45.2 | CVE-2022-3099  | HIGH             | 7.8        | Use After Free in GitHub repository vim/vim prior to 9.0.0360.   |
| Git | 2.45.2 | CVE-2022-3123  | MEDIUM           | 6.1        | Cross-site Scripting (XSS) - Reflected in GitHub repository splitbrain/dokuwiki prior to 2022-07-31a.  |
| Git | 2.45.2 | CVE-2022-3127  | MEDIUM           | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 20.2.8.  |
| Git | 2.45.2 | CVE-2022-2901  | HIGH             | 7.1        | Improper Authorization in GitHub repository chatwoot/chatwoot prior to 2.8.  |
| Git | 2.45.2 | CVE-2022-2714  | CRITICAL         | 9.8        | Improper Handling of Length Parameter Inconsistency in GitHub repository francoisjacquet/rosariosis prior to 10.0.   |
| Git | 2.45.2 | CVE-2022-3134  | HIGH             | 7.8        | Use After Free in GitHub repository vim/vim prior to 9.0.0389.   |

|     |        |                |                  |            |  |
|-----|--------|----------------|------------------|------------|--|
| Git | 2.45.2 | CVE-2022-3152  | HIGH             | 8.8        | Unverified Password Change in GitHub repository phpfusion/phpfusion prior to 9.10.20.  |
| Git | 2.45.2 | CVE-2022-36069 | ['HIGH', 'HIGH'] | [7.3, 7.3] | Poetry is a dependency manager for Python. When handling dependencies that come from a Git repository instead of a registry, Poetry uses various commands, such as `git clone`. These commands are constructed using user input (e.g. the repository URL). When building the commands, Poetry correctly avoids Command Injection vulnerabilities by passing an array of arguments instead of a command string. However, there is the possibility that a user input starts with a dash (`-`) and is therefore treated as an optional argument instead of a positional one. This can lead to Code Execution because some of the commands have options that can be leveraged to run arbitrary executables. If a developer is exploited, the attacker could steal credentials or persist their access. If the exploit happens on a server, the attackers could use their access to attack other internal systems. Since this vulnerability requires a fair amount of user interaction, it is not as dangerous as a remotely exploitable o... |
| Git | 2.45.2 | CVE-2022-36070 | ['HIGH', 'HIGH'] | [7.3, 7.3] | Poetry is a dependency manager for Python. To handle dependencies that come from a Git repository, Poetry executes various commands, e.g. `git config`. These commands are being executed using the executable's name and not its absolute path. This can lead to the execution of untrusted code due to the way Windows resolves executable names to paths. Unlike Linux-based operating systems, Windows searches for the executable in the current directory first and looks in the paths that are defined in the `PATH` environment variable afterward. This vulnerability can lead to Arbitrary Code Execution, which would lead to the takeover of the system. If a developer is exploited, the attacker could steal credentials or persist their access. If the exploit happens on a server, the attackers could use their access to attack other internal systems. Since this vulnerability requires a fair amount of user interaction, it is not as dangerous as a remotely exploitable one. However, it still puts develo...   |
| Git | 2.45.2 | CVE-2022-3138  | MEDIUM           | 6.1        | Cross-site Scripting (XSS) - Generic in GitHub repository jgraph/drawio prior to 20.3.0.   |
| Git | 2.45.2 | CVE-2022-3148  | MEDIUM           | 6.1        | Cross-site Scripting (XSS) - Generic in GitHub repository jgraph/drawio prior to 20.3.0.   |
| Git | 2.45.2 | CVE-2022-3153  | MEDIUM           | 5.5        | NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0404.   |

|     |        |                |                          |            |  |
|-----|--------|----------------|--------------------------|------------|--|
| Git | 2.45.2 | CVE-2022-3167  | HIGH                     | 8.8        | Improper Restriction of Rendered UI Layers or Frames in GitHub repository ikus060/rdiffweb prior to 2.4.1.   |
| Git | 2.45.2 | CVE-2022-2925  | MEDIUM                   | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository appwrite/appwrite prior to 1.0.0-RC1.   |
| Git | 2.45.2 | CVE-2022-3133  | HIGH                     | 7.8        | OS Command Injection in GitHub repository jgraph/drawio prior to 20.3.0.   |
| Git | 2.45.2 | CVE-2022-25295 | ['MEDIUM', 'MEDIUM']     | [5.4, 5.4] | This affects the package github.com/gophish/gophish before 0.12.0. The Open Redirect vulnerability exists in the next query parameter. The application uses url.Parse(r.FormValue("next")) to extract path and eventually redirect user to a relative URL, but if next parameter starts with multiple backslashes like \\\\\\\example.com, browser will redirect user to http://example.com.   |
| Git | 2.45.2 | CVE-2022-3178  | HIGH                     | 7.8        | Buffer Over-read in GitHub repository gpac/gpac prior to 2.1.0-DEV.  |
| Git | 2.45.2 | CVE-2022-3174  | HIGH                     | 7.5        | Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository ikus060/rdiffweb prior to 2.4.2.   |
| Git | 2.45.2 | CVE-2022-3175  | MEDIUM                   | 5.3        | Missing Custom Error Page in GitHub repository ikus060/rdiffweb prior to 2.4.2.  |
| Git | 2.45.2 | CVE-2022-3179  | HIGH                     | 8.8        | Weak Password Requirements in GitHub repository ikus060/rdiffweb prior to 2.4.2.   |
| Git | 2.45.2 | CVE-2022-39205 | ['CRITICAL', 'CRITICAL'] | [9.0, 9.8] | Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. In versions of Onedev prior to 7.3.0 unauthenticated users can take over a OneDev instance if there is no properly configured reverse proxy. The /git-prereceive-callback endpoint is used by the pre-receive git hook on the server to check for branch protections during a push event. It is only intended to be accessed from localhost, but the check relies on the X-Forwarded-For header. Invoking this endpoint leads to the execution of one of various git commands. The environment variables of this command execution can be controlled via query parameters. This allows attackers to write to arbitrary files, which can in turn lead to the execution of arbitrary code. Such an attack would be very hard to detect, which increases the potential impact even more. Users are advised to upgrade. There are no known workarounds for this issue. |

|     |        |                |                          |            |   |
|-----|--------|----------------|--------------------------|------------|---|
| Git | 2.45.2 | CVE-2022-39206 | ['CRITICAL', 'CRITICAL'] | [9.9, 9.9] | <p>Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. When using Docker-based job executors, the Docker socket (e.g. /var/run/docker.sock on Linux) is mounted into each Docker step. Users that can define and trigger CI/CD jobs on a project could use this to control the Docker daemon on the host machine. This is a known dangerous pattern, as it can be used to break out of Docker containers and, in most cases, gain root privileges on the host system. This issue allows regular (non-admin) users to potentially take over the build infrastructure of a OneDev instance. Attackers need to have an account (or be able to register one) and need permission to create a project. Since code.onedev.io has the right preconditions for this to be exploited by remote attackers, it could have been used to hijack builds of OneDev itself, e.g. by injecting malware into the docker images that are built and pushed to Docker Hub. The impact is increased by this as described before. Users are...</p> |
| Git | 2.45.2 | CVE-2022-39207 | ['MEDIUM', 'MEDIUM']     | [5.4, 5.4] | <p>Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. During CI/CD builds, it is possible to save build artifacts for later retrieval. They can be accessed through OneDev's web UI after the successful run of a build. These artifact files are served by the webserver in the same context as the UI without any further restrictions. This leads to Cross-Site Scripting (XSS) when a user creates a build artifact that contains HTML. When accessing the artifact, the content is rendered by the browser, including any JavaScript that it contains. Since all cookies (except for the rememberMe one) do not set the HttpOnly flag, an attacker could steal the session of a victim and use it to impersonate them. To exploit this issue, attackers need to be able to modify the content of artifacts, which usually means they need to be able to modify a project's build spec. The exploitation requires the victim to click on an attacker's link. It can be used to elevate privileges by targeting ...</p> |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-39208 | ['HIGH', 'HIGH']     | [7.5, 7.5] | Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. All files in the /opt/onedev/sites/ directory are exposed and can be read by unauthenticated users. This directory contains all projects, including their bare git repos and build artifacts. This file disclosure vulnerability can be used by unauthenticated attackers to leak all project files of any project. Since project IDs are incremental, an attacker could iterate through them and leak all project data. This issue has been resolved in version 7.3.0 and users are advised to upgrade. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-2900  | CRITICAL             | 9.1        | Server-Side Request Forgery (SSRF) in GitHub repository ionicabizau/parse-url prior to 8.1.0.   |
| Git | 2.45.2 | CVE-2022-36056 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Cosign is a project under the sigstore organization which aims to make signatures invisible infrastructure. In versions prior to 1.12.0 a number of vulnerabilities have been found in cosign verify-blob, where Cosign would successfully verify an artifact when verification should have failed. First a cosign bundle can be crafted to successfully verify a blob even if the embedded rekorBundle does not reference the given signature. Second, when providing identity flags, the email and issuer of a certificate is not checked when verifying a Rekor bundle, and the GitHub Actions identity is never checked. Third, providing an invalid Rekor bundle without the experimental flag results in a successful verification. And fourth an invalid transparency log entry will result in immediate success for verification. Details and examples of these issues can be seen in the GHSA-8gw7-4j42-w388 advisory linked. Users are advised to upgrade to 1.12.0. There are no known workarounds for these issues. |
| Git | 2.45.2 | CVE-2022-3221  | HIGH                 | 8.8        | Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.3.   |
| Git | 2.45.2 | CVE-2022-3222  | MEDIUM               | 5.5        | Uncontrolled Recursion in GitHub repository gpac/gpac prior to 2.1.0-DEV.   |
| Git | 2.45.2 | CVE-2022-3224  | MEDIUM               | 6.1        | Misinterpretation of Input in GitHub repository ionicabizau/parse-url prior to 8.1.0.   |
| Git | 2.45.2 | CVE-2022-3211  | MEDIUM               | 5.4        | Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.6.   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-39209 | ['HIGH', 'MEDIUM'] | [7.5, 6.5] | cmark-gfm is GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C. In versions prior to 0.29.0.gfm.6 a polynomial time complexity issue in cmark-gfm's autolink extension may lead to unbounded resource exhaustion and subsequent denial of service. Users may verify the patch by running <code>`python3 -c 'print("![" 100000 + "\n")'   ./cmark-gfm -e autolink`</code> , which will resource exhaust on unpatched cmark-gfm but render correctly on patched cmark-gfm. This vulnerability has been patched in 0.29.0.gfm.6. Users are advised to upgrade. Users unable to upgrade should disable the use of the autolink extension. |
| Git | 2.45.2 | CVE-2022-3223  | MEDIUM             | 6.1        | Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 20.3.1.   |
| Git | 2.45.2 | CVE-2022-3225  | ['HIGH', 'MEDIUM'] | [8.8, 5.7] | Improper Control of Dynamically-Managed Code Resources in GitHub repository budibase/budibase prior to 1.3.20.  |
| Git | 2.45.2 | CVE-2022-35934 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of <code>tf.reshape</code> op in TensorFlow is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by overflowing the number of elements in a tensor. This issue has been patched in GitHub commit 61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35935 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of <code>SobolSampleOp</code> is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by assuming <code>`input(0)`</code> , <code>`input(1)`</code> , and <code>`input(2)`</code> to be scalar. This issue has been patched in GitHub commit c65c67f88ad770662e8f191269a907bf2b94b1bf. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                |

|     |        |                |                      |            |   |
|-----|--------|----------------|----------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35937 | ['HIGH', 'CRITICAL'] | [7.0, 9.1] | TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read is triggered. This issue has been patched in GitHub commit 595a65a3e224a0362d7e68c2213acfc2b499a196. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                     |
| Git | 2.45.2 | CVE-2022-35938 | ['HIGH', 'CRITICAL'] | [7.0, 9.1] | TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. This issue has been patched in GitHub commit 4142e47e9e31db481781b955ed3ff807a781b494. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.          |
| Git | 2.45.2 | CVE-2022-35939 | ['HIGH', 'CRITICAL'] | [7.0, 9.8] | TensorFlow is an open source platform for machine learning. The `ScatterNd` function takes an input argument that determines the indices of the output tensor. An input index greater than the output tensor or less than zero will either write content at the wrong index or trigger a crash. We have patched the issue in GitHub commit b4d4b4cb019bd7240a52daa4ba61e3cc814f0384. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-35940 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The `RaggedRangOp` function takes an argument `limits` that is eventually used to construct a `TensorShape` as an `int64`. If `limits` is a very large float, it can overflow when converted to an `int64`. This triggers an `InvalidArgument` but also throws an abort signal that crashes the program. We have patched the issue in GitHub commit 37cefa91bee4eace55715eeef43720b958a01192. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35941 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The `AvgPoolOp` function takes an argument `ksize` that must be positive but is not checked. A negative `ksize` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds to this issue.  |
| Git | 2.45.2 | CVE-2022-35952 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The `UnbatchGradOp` function takes an argument `id` that is assumed to be a scalar. A nonscalar `id` can trigger a `CHECK` failure and crash the program. It also requires its argument `batch_index` to contain three times the number of elements as indicated in its `batch_index.dim_size(0)`. An incorrect `batch_index` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 5f945fc6409a3c1e90d6970c9292f805f6e6ddf2. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-35959 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of <code>`AvgPool3DGradOp`</code> does not fully validate the input <code>`orig_input_shape`</code> . This results in an overflow that results in a <code>`CHECK`</code> failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 9178ac9d6389bdc54638ab913ea0e419234d14eb. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35960 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. In <code>`core/kernels/list_kernels.cc`</code> 's <code>TensorListReserve`</code> , <code>`num_elements`</code> is assumed to be a tensor of size 1. When a <code>`num_elements`</code> of more than 1 element is provided, then <code>`tf.raw_ops.TensorListReserve`</code> fails the <code>`CHECK_EQ`</code> in <code>`CheckIsAlignedAndSingleElement`</code> . We have patched the issue in GitHub commit b5f6fbfa76576202b72119897561e3bd4f179c7. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35963 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of <code>`FractionalAvgPoolGrad`</code> does not fully validate the input <code>`orig_input_tensor_shape`</code> . This results in an overflow that results in a <code>`CHECK`</code> failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 03a659d7be9a1154fdf5eeac221e5950fec07dad. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.  |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-35964 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of `BlockLSTMGradV2` does not fully validate its inputs. This results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 2a458fc4866505be27c62f81474ecb2b870498fa. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                               |
| Git | 2.45.2 | CVE-2022-35965 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `LowerBound` or `UpperBound` is given an empty `sorted_inputs` input, it results in a `nullptr` dereference, leading to a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bce3717eae4f769019fd18e990464ca4a2efeea. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35966 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizedAvgPool` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7cdf9d4d2083b739ec81cfda546b0c99f50622. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                          |
| Git | 2.45.2 | CVE-2022-35967 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizedAdd` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                            |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-35968 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of `AvgPoolGrad` does not fully validate the input `orig_input_shape`. This results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35969 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. The implementation of `Conv2DBackpropInput` requires `input_sizes` to be 4-dimensional. Otherwise, it gives a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 50156d547b9a1da0144d7babe665cf690305b33c. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35970 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizedInstanceNorm` is given `x_min` or `x_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                     |
| Git | 2.45.2 | CVE-2022-35971 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVars` is given `min` or `max` tensors of a nonzero rank, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35972 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizedBiasAdd` is given `min_input`, `max_input`, `min_bias`, `max_bias` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35973 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizedMatMul` is given nonscalar input for: `min_a`, `max_a`, `min_b`, or `max_b` It gives a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit aca766ac7693bf29ed0df55ad6bfcc78f35e7f48. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                        |
| Git | 2.45.2 | CVE-2022-35974 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizeDownAndShrinkRange` is given nonscalar inputs for `input_min` or `input_max`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 73ad1815ebcf7c051f9c2f7ab5024380ca8613. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                    |
| Git | 2.45.2 | CVE-2022-35979 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizedRelu` or `QuantizedRelu6` are given nonscalar inputs for `min_features` or `max_features`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.    |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-35981 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. `FractionalMaxPoolGrad` validates its inputs with `CHECK` failures instead of with returning errors. If it gets incorrectly sized inputs, the `CHECK` failure can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 8741e57d163a079db05a7107a7609af70931def4. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35982 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `SparseBincount` is given inputs for `indices`, `values`, and `dense_shape` that do not make a valid sparse tensor, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 40adbe4dd15b582b0210dfbf40c243a62f5119fa. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.          |
| Git | 2.45.2 | CVE-2022-35983 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `Save` or `SaveSlices` is run over tensors of an unsupported `dtype`, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.  |
| Git | 2.45.2 | CVE-2022-35984 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. `ParameterizedTruncatedNormal` assumes `shape` is of type `int32`. A valid `shape` of type `int64` results in a mismatched type `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 72180be03447a10810edca700cbc9af690dfb51. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.              |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35985 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `LRNGrad` is given an `output_image` input tensor that is not 4-D, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bd90b3efab4ec958b228cd7cfe9125be1c0cf255. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.  |
| Git | 2.45.2 | CVE-2022-35986 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `RaggedBincount` is given an empty input tensor `splits`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7a4591fd4f065f4fa903593bc39b2f79530a74b8. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35987 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. `DenseBincount` assumes its input tensor `weights` to either have the same shape as its input tensor `input` or to be length-0. A different `weights` shape will trigger a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf4c14353c2328636a18bfad1e151052c81d5f43. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35988 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `tf.linalg.matrix_rank` receives an empty input `a`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-35989 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `MaxPool` receives a window size input array `ksize` with dimensions greater than its input tensor `input`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 32d7bd3defd134f21a4e344c8dfd40099aaf6b18. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35990 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_per_channel_gradient` receives input `min` or `max` of rank other than 1, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319fed. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.             |
| Git | 2.45.2 | CVE-2022-36018 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `RaggedTensorToVariant` is given a `rt_nested_splits` list that contains tensors of ranks other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 88f93dfe691563baa4ae1e80ccde2d5c7a143821. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.            |
| Git | 2.45.2 | CVE-2022-36019 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVarsPerChannel` is given `min` or `max` tensors of a rank other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                        |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-36026 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `QuantizeAndDequantizeV3` is given a nonscalar `num_bits` input tensor, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit f3f9cb38ecfe5a8a703f2c4a8fead434ef291713. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                 |
| Git | 2.45.2 | CVE-2022-35991 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `TensorListScatter` and `TensorListScatterV2` receive an `element_shape` of a rank greater than one, they give a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit bb03fdf4aae944ab2e4b35c7daa051068a8b7f61. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35992 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `TensorListFromTensor` receives an `element_shape` of a rank greater than one, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 3db59a042a38f4338aa207922fa2f476e000a6ee. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                        |
| Git | 2.45.2 | CVE-2022-35993 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `SetSize` receives an input `set_shape` that is not a 1D tensor, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit cf70b79d2662c0d3c6af74583641e345fc939467. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                          |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35994 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `CollectiveGather` receives an scalar input `input`, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c1f491817dec39a26be3c574e86a88c30f3c4770. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35995 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `AudioSummaryV2` receives an input `sample_rate` with more than one element, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf6b45244992e2ee543c258e519489659c99fb7f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-35996 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `Conv2D` is given empty `input` and the `filter` and `padding` sizes are valid, the output is all-zeros. This causes division-by-zero floating point exceptions that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 611d80db29dd7b0cfb755772c69d60ae5bca05f9. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-35997 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `tf.sparse.cross` receives an input `separator` that is not a scalar, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 83dcb4dbfa094e33db084e97c4d0531a559e0ebf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-35998 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `EmptyTensorList` receives an input `element_shape` with more than one dimension, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c8ba76d48567aed347508e0552a257641931024d. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.  |
| Git | 2.45.2 | CVE-2022-35999 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `Conv2DBackpropInput` receives empty `out_backprop` inputs (e.g. `[3, 1, 0, 1]`), the current CPU/GPU kernels `CHECK` fail (one with dnnl, the other with cudnn). This can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 27a65a43cf763897fecfa5c5db5cc653fc5dd0346. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-36000 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `mlir::tf::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit aed36912609fc07229b4d0a7b44f3f48efc00fd0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-36001 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `DrawBoundingBoxes` receives an input `boxes` that is not of dtype `float`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit da0d65cdc1270038e72157ba35bf74b85d9bda11. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-36002 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `Unbatch` receives a nonscalar input `id`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 4419d10d576adefa36b0e0a9425d2569f7c0189f. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-36003 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `RandomPoissonV2` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfcd6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-36004 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `tf.random.gamma` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfcd6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-36005 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_gradient` receives input `min` or `max` that is nonscalar, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |

|     |        |                |                    |            |  |
|-----|--------|----------------|--------------------|------------|--|
| Git | 2.45.2 | CVE-2022-36011 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit 1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.         |
| Git | 2.45.2 | CVE-2022-36012 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it crashes. We have patched the issue in GitHub commit ad069af92392efee1418c48ff561fd3070a03d7b. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                          |
| Git | 2.45.2 | CVE-2022-36013 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `mlir::tfg::GraphDefImporter::ConvertNodeDef` tries to convert NodeDefs without an op name, it crashes. We have patched the issue in GitHub commit a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                   |
| Git | 2.45.2 | CVE-2022-36014 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `mlir::tfg::TFOp::nameAttr` receives null type list attributes, it crashes. We have patched the issue in GitHub commits 3a754740d5414e362512ee981eefba41561a63a6 and a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |

|     |        |                |                    |            |   |
|-----|--------|----------------|--------------------|------------|---|
| Git | 2.45.2 | CVE-2022-36015 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `RangeSize` receives values that do not fit into an `int64_t`, it crashes. We have patched the issue in GitHub commit 37e64539cd29fcfb814c4451152a60f5d107b0f0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |
| Git | 2.45.2 | CVE-2022-36016 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When `tensorflow::full_type::SubstituteFromAttrs` receives a `FullTypeDef& t` that is not exactly three args, it triggers a `CHECK`-fail instead of returning a status. We have patched the issue in GitHub commit 6104f0d4091c260ce9352f9155f7e9b725eab012. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.                                       |
| Git | 2.45.2 | CVE-2022-36017 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. If `Requantize` is given `input_min`, `input_max`, `requested_output_min`, `requested_output_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-36027 | ['MEDIUM', 'HIGH'] | [5.9, 7.5] | TensorFlow is an open source platform for machine learning. When converting transposed convolutions using per-channel weight quantization the converter segfaults and crashes the Python process. We have patched the issue in GitHub commit aa0b852a4588cea4d36b74feb05d93055540b450. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.   |

|     |        |                |                           |               |   |
|-----|--------|----------------|---------------------------|---------------|---|
| Git | 2.45.2 | CVE-2022-39217 | ['MEDIUM',<br>'CRITICAL'] | [5.8,<br>9.8] | some-natalie/ghas-to-csv (GitHub Advanced Security to CSV) is a GitHub action which scrapes the GitHub Advanced Security API and shoves it into a CSV. In affected versions this GitHub Action creates a CSV file without sanitizing the output of the APIs. If an alert is dismissed or any other custom field contains executable code / formulas, it might be run when an endpoint opens that CSV file in a spreadsheet program. This issue has been addressed in version `v1`. Users are advised to use `v1` or later. There are no known workarounds for this issue. |
| Git | 2.45.2 | CVE-2022-3173  | MEDIUM                    | 4.3           | Improper Authentication in GitHub repository snipe/snipe-it prior to 6.0.10.  |
| Git | 2.45.2 | CVE-2022-3231  | MEDIUM                    | 5.4           | Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.9.0.   |
| Git | 2.45.2 | CVE-2022-3232  | MEDIUM                    | 4.3           | Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.5.   |
| Git | 2.45.2 | CVE-2022-3234  | HIGH                      | 7.8           | Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0483.  |
| Git | 2.45.2 | CVE-2022-3235  | HIGH                      | 7.8           | Use After Free in GitHub repository vim/vim prior to 9.0.0490.  |
| Git | 2.45.2 | CVE-2022-2924  | MEDIUM                    | 5.4           | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.3.  |
| Git | 2.45.2 | CVE-2022-3000  | MEDIUM                    | 5.4           | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.  |
| Git | 2.45.2 | CVE-2022-3004  | MEDIUM                    | 5.4           | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.  |
| Git | 2.45.2 | CVE-2022-3005  | MEDIUM                    | 5.4           | Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0.  |
| Git | 2.45.2 | CVE-2022-3242  | MEDIUM                    | 6.1           | Code Injection in GitHub repository microweber/microweber prior to 1.3.2.   |
| Git | 2.45.2 | CVE-2022-2872  | MEDIUM                    | 5.4           | Unrestricted Upload of File with Dangerous Type in GitHub repository octoprint/octoprint prior to 1.8.3.  |
| Git | 2.45.2 | CVE-2022-3068  | HIGH                      | 8.8           | Improper Privilege Management in GitHub repository octoprint/octoprint prior to 1.8.3.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2007-0045 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distributed with Adobe Reader 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2, for Mozilla Firefox, Microsoft Internet Explorer 6 SP1, Google Chrome, Opera 8.5.4 build 770, and Opera 9.10.8679 on Windows allow remote attackers to inject arbitrary JavaScript and conduct other attacks via a .pdf URL with a javascript: or res: URI with (1) FDF, (2) XML, and (3) XFDF AJAX parameters, or (4) an arbitrarily named name=URI anchor identifier, aka "Universal XSS (UXSS)." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2007-0048 | None | None | Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distributed with Adobe Reader 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2, when used with Internet Explorer, Google Chrome, or Opera, allows remote attackers to cause a denial of service (memory consumption) via a long sequence of # (hash) characters appended to a PDF URL, related to a "cross-site scripting issue."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-4340 | None | None | Google Chrome 0.2.149.29 and 0.2.149.30 allows remote attackers to cause a denial of service (memory consumption) via an HTML document containing a carriage return ("\\r\\n\\r\\n") argument to the window.open function.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-4724 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome 0.2.149.30 allow remote attackers to inject arbitrary web script or HTML via an ftp:// URL for an HTML document within a (1) JPG, (2) PDF, or (3) TXT file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-5749 | None | None | Argument injection vulnerability in Google Chrome 1.0.154.36 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI. NOTE: a third party disputes this issue, stating that Chrome "will ask for user permission" and "cannot launch the applet even [if] you have given out the permission."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-5915 | None | None | An unspecified function in the JavaScript implementation in Google Chrome creates and exposes a "temporary footprint" when there is a current login to a web site, which makes it easier for remote attackers to trick a user into acting upon a spoofed pop-up message, aka an "in-session phishing attack." NOTE: as of 20090116, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-0374 | None | None | Google Chrome 1.0.154.43 allows remote attackers to trick a user into visiting an arbitrary URL via an onclick action that moves a crafted element to the current mouse position, related to a "Clickjacking" vulnerability. NOTE: a third party disputes the relevance of this issue, stating that "every sufficiently featured browser is and likely will remain susceptible to the behavior known as clickjacking," and adding that the exploit code "is not a valid demonstration of the issue.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-0276 | None | None | Cross-domain vulnerability in the V8 JavaScript engine in Google Chrome before 1.0.154.46 allows remote attackers to bypass the Same Origin Policy via a crafted script that accesses another frame and reads its full URL and possibly other sensitive information, or modifies the URL of this frame.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-0411 | None | None | Google Chrome before 1.0.154.46 does not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls and other web script.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1412 | None | None | Argument injection vulnerability in the chromehtml: protocol handler in Google Chrome before 1.0.154.59, when invoked by Internet Explorer, allows remote attackers to determine the existence of files, and open tabs for URLs that do not satisfy the IsWebSafeScheme restriction, via a web page that sets document.location to a chromehtml: value, as demonstrated by use of a (1) javascript: or (2) data: URL. NOTE: this can be leveraged for Universal XSS by exploiting certain behavior involving persistence across page transitions. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1413 | None | None | Google Chrome 1.0.x does not cancel timeouts upon a page transition, which makes it easier for attackers to conduct Universal XSS attacks by calling setTimeout to trigger future execution of JavaScript code, and then modifying document.location to arrange for JavaScript execution in the context of an arbitrary web site. NOTE: this can be leveraged for a remote attack by exploiting a chromehtml: argument-injection vulnerability.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1414 | None | None | Google Chrome 2.0.x lets modifications to the global object persist across a page transition, which makes it easier for attackers to conduct Universal XSS attacks via unspecified vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1514 | None | None | Google Chrome 1.0.154.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a throw statement with a long exception value.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1441 | None | None | Heap-based buffer overflow in the ParamTraits<SkBitmap>::Read function in Google Chrome before 1.0.154.64 allows attackers to leverage renderer access to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to a large bitmap that arrives over the IPC channel.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1442 | None | None | Multiple integer overflows in Skia, as used in Google Chrome 1.x before 1.0.154.64 and 2.x, and possibly Android, might allow remote attackers to execute arbitrary code in the renderer process via a crafted (1) image or (2) canvas.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1598 | None | None | Google Chrome executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-0945 | None | None | Array index error in the insertItemBefore method in WebKit, as used in Apple Safari before 3.2.3 and 4 Public Beta, iPhone OS 1.0 through 2.2.1, iPhone OS for iPod touch 1.1 through 2.2.1, Google Chrome Stable before 1.0.154.65, and possibly other products allows remote attackers to execute arbitrary code via a document with a SVGPathList data structure containing a negative index in the (1) SVGTransformList, (2) SVGStringList, (3) SVGNumberList, (4) SVGPathSegList, (5) SVGPointList, or (6) SVGLengthList SVGList object, which triggers memory corruption. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-1690 | None | None | Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.0, iPhone OS 1.0 through 2.2.1, iPhone OS for iPod touch 1.1 through 2.2.1, Google Chrome 1.0.154.53, and possibly other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) by setting an unspecified property of an HTML tag that causes child elements to be freed and later accessed when an HTML error occurs, related to "recursion in certain DOM event handlers."   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2060 | None | None | src/net/http/http_transaction_winhttp.cc in Google Chrome before 1.0.154.53 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2068 | None | None | Google Chrome detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2071 | None | None | Google Chrome before 1.0.154.53 displays a cached certificate for a (1) 4xx or (2) 5xx CONNECT response page returned by a proxy server, which allows man-in-the-middle attackers to spoof an arbitrary https site by letting a browser obtain a valid certificate from this site during one request, and then sending the browser a crafted 502 response page upon a subsequent request.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2121 | None | None | Buffer overflow in the browser kernel in Google Chrome before 2.0.172.33 allows remote HTTP servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted response.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2352 | None | None | Google Chrome 1.0.154.48 and earlier does not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header, a related issue to CVE-2009-1312. NOTE: it was later reported that 2.0.172.28, 2.0.172.37, and 3.0.193.2 Beta are also affected. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2555 | None | None | Heap-based buffer overflow in src/jsregexp.cc in Google V8 before 1.1.10.14, as used in Google Chrome before 2.0.172.37, allows remote attackers to execute arbitrary code in the Chrome sandbox via a crafted JavaScript regular expression.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2556 | None | None | Google Chrome before 2.0.172.37 allows attackers to leverage renderer access to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger excessive memory allocation.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2578 | None | None | Google Chrome 2.x through 2.0.172 allows remote attackers to cause a denial of service (application crash) via a long Unicode string argument to the write method, a related issue to CVE-2009-2479.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-6994 | None | None | Stack-based buffer overflow in the SaveAs feature (SaveFileAsWithFilter function) in win_util.cc in Google Chrome 0.2.149.27 allows user-assisted remote attackers to execute arbitrary code via a web page with a long TITLE element, which triggers the overflow when the user saves the page and a long filename is generated. NOTE: it might be possible to exploit this issue via an HTTP response that includes a long filename in a Content-Disposition header. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-6995 | None | None | Integer underflow in net/base/escape.cc in chrome.dll in Google Chrome 0.2.149.27 allows remote attackers to cause a denial of service (browser crash) via a URI with an invalid handler followed by a "%" (percent) character, which triggers a buffer over-read, as demonstrated using an "about:%" URI.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-6996 | None | None | Google Chrome BETA (0.2.149.27) does not prompt the user before saving an executable file, which makes it easier for remote attackers or malware to cause a denial of service (disk consumption) or exploit other vulnerabilities via a URL that references an executable file, possibly related to the "ask where to save each file before downloading" setting.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-6997 | None | None | Google Chrome 0.2.149.27 allows user-assisted remote attackers to cause a denial of service (browser crash) via an IMG tag with a long src attribute, which triggers the crash when the victim performs an "Inspect Element" action.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-6998 | None | None | Stack-based buffer overflow in chrome/common/gfx/url_elider.cc in Google Chrome 0.2.149.27 and other versions before 0.2.149.29 might allow user-assisted remote attackers to execute arbitrary code via a link target (href attribute) with a large number of path elements, which triggers the overflow when the status bar is updated after the user hovers over the link.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2955 | None | None | Google Chrome 1.0.154.48 and earlier allows remote attackers to cause a denial of service (CPU consumption and application hang) via JavaScript code with a long string value for the hash property (aka location.hash), a related issue to CVE-2008-5715.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-7061 | None | None | The tooltip manager (chrome/views/tooltip_manager.cc) in Google Chrome 0.2.149.29 Build 1798 and possibly other versions before 0.2.149.30 allows remote attackers to cause a denial of service (CPU consumption or crash) via a tag with a long title attribute, which is not properly handled when displaying a tooltip, a different vulnerability than CVE-2008-6994. NOTE: there is inconsistent information about the environments under which this issue exists.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2935 | None | None | Google V8, as used in Google Chrome before 2.0.172.43, allows remote attackers to bypass intended restrictions on reading memory, and possibly obtain sensitive information or execute arbitrary code in the Chrome sandbox, via crafted JavaScript.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2973 | None | None | Google Chrome before 2.0.172.43 does not prevent SSL connections to a site with an X.509 certificate signed with the (1) MD2 or (2) MD4 algorithm, which makes it easier for man-in-the-middle attackers to spoof arbitrary HTTPS servers via a crafted certificate, a related issue to CVE-2009-2409.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2974 | None | None | Google Chrome 1.0.154.65, 1.0.154.48, and earlier allows remote attackers to (1) cause a denial of service (application hang) via vectors involving a chromehtml: URI value for the document.location property or (2) cause a denial of service (application hang and CPU consumption) via vectors involving a series of function calls that set a chromehtml: URI value for the document.location property.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3011 | None | None | Google Chrome 1.0.154.48 and earlier, 2.0.172.28, 2.0.172.37, and 3.0.193.2 Beta does not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: the JavaScript executes outside of the context of the HTTP site. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-7246 | None | None | Google Chrome 0.2.149.29 and earlier allows remote attackers to cause a denial of service (unusable browser) by calling the window.print function in a loop, aka a "printing DoS attack," possibly a related issue to CVE-2009-0821.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3263 | None | None | Cross-site scripting (XSS) vulnerability in Google Chrome 2.x and 3.x before 3.0.195.21 allows remote attackers to inject arbitrary web script or HTML via a (1) RSS or (2) Atom feed, related to the rendering of the application/rss+xml content type as XML "active content."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3264 | None | None | The getSVGDocument method in Google Chrome before 3.0.195.21 omits an unspecified "access check," which allows remote web servers to bypass the Same Origin Policy and conduct cross-site scripting attacks via unknown vectors, related to a user's visit to a different web server that hosts an SVG document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3268 | None | None | Google Chrome 1.0.154.48 and earlier allows remote attackers to cause a denial of service (CPU consumption) via an automatically submitted form containing a KEYGEN element, a related issue to CVE-2009-1828.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3456 | None | None | Google Chrome, possibly 3.0.195.21 and earlier, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3931 | None | None | Incomplete blacklist vulnerability in browser/download/download_exe.cc in Google Chrome before 3.0.195.32 allows remote attackers to force the download of certain dangerous files via a "Content-Disposition: attachment" designation, as demonstrated by (1) .mht and (2) .mhtml files, which are automatically executed by Internet Explorer 6; (3) .svg files, which are automatically executed by Safari; (4) .xml files; (5) .htt files; (6) .xsl files; (7) .xslt files; and (8) image files that are forbidden by the victim's site policy. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3932 | None | None | The Gears plugin in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service (memory corruption and plugin crash) or possibly execute arbitrary code via unspecified use of the Gears SQL API, related to putting "SQL metadata into a bad state."  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3933 | None | None | WebKit before r50173, as used in Google Chrome before 3.0.195.32, allows remote attackers to cause a denial of service (CPU consumption) via a web page that calls the JavaScript setInterval method, which triggers an incompatibility between the WTF::currentTime and base::Time functions.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-3934 | None | None | The WebFrameLoaderClient::dispatchDidChangeLocationWithinPage function in src/webkit/glue/webframeloaderclient_impl.cc in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service via a page-local link, related to an "empty redirect chain," as demonstrated by a message in Yahoo! Mail.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2009-2816 | None | None | The implementation of Cross-Origin Resource Sharing (CORS) in WebKit, as used in Apple Safari before 4.0.4 and Google Chrome before 3.0.195.33, includes certain custom HTTP headers in the OPTIONS request during cross-origin operations with preflight, which makes it easier for remote attackers to conduct cross-site request forgery (CSRF) attacks via a crafted web page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0315 | None | None | WebKit before r53607, as used in Google Chrome before 4.0.249.89, allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then reading the document.styleSheets[0].href property value, related to an IFRAME element.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0556 | None | None | browser/login/login_prompt.cc in Google Chrome before 4.0.249.89 populates an authentication dialog with credentials that were stored by Password Manager for a different web site, which allows user-assisted remote HTTP servers to obtain sensitive information via a URL that requires authentication, as demonstrated by a URL in the SRC attribute of an IMG element.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0643 | None | None | Google Chrome before 4.0.249.89 attempts to make direct connections to web sites when all configured proxy servers are unavailable, which allows remote HTTP servers to obtain potentially sensitive information about the identity of a client user via standard HTTP logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.                |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0644 | None | None | Google Chrome before 4.0.249.89, when a SOCKS 5 proxy server is configured, sends DNS queries directly, which allows remote DNS servers to obtain potentially sensitive information about the identity of a client user via request logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0645 | None | None | Multiple integer overflows in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0646 | None | None | Multiple integer signedness errors in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0647 | None | None | WebKit before r53525, as used in Google Chrome before 4.0.249.89, allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed RUBY element, as demonstrated by a <ruby>><table><rt> sequence.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0649 | None | None | Integer overflow in the CrossCallParamsEx::CreateFromBuffer function in sandbox/src/crosscall_server.cc in Google Chrome before 4.0.249.89 allows attackers to leverage renderer access to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a malformed message, related to deserializing of sandbox messages. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0650 | None | None | WebKit, as used in Google Chrome before 4.0.249.78 and Apple Safari, allows remote attackers to bypass intended restrictions on popup windows via crafted use of a mouse click event.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0651 | None | None | WebKit before r52784, as used in Google Chrome before 4.0.249.78 and Apple Safari before 4.0.5, permits cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type and the stylesheet document is malformed, which allows remote attackers to obtain sensitive information via a crafted document.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0655 | None | None | Use-after-free vulnerability in Google Chrome before 4.0.249.78 allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving the display of a blocked popup window during navigation to a different web site.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0656 | None | None | WebKit before r51295, as used in Google Chrome before 4.0.249.78, presents a directory-listing page in response to an XMLHttpRequest for a file:/// URL that corresponds to a directory, which allows attackers to obtain sensitive information or possibly have unspecified other impact via a crafted local HTML document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0657 | None | None | Google Chrome before 4.0.249.78 on Windows does not perform the expected encoding, escaping, and quoting for the URL in the --app argument in a desktop shortcut, which allows user-assisted remote attackers to execute arbitrary programs or obtain sensitive information by tricking a user into creating a crafted shortcut.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0658 | None | None | Multiple integer overflows in Skia, as used in Google Chrome before 4.0.249.78, allow remote attackers to execute arbitrary code in the Chrome sandbox or cause a denial of service (memory corruption and application crash) via vectors involving CANVAS elements.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0659 | None | None | The image decoder in WebKit before r52833, as used in Google Chrome before 4.0.249.78, does not properly handle a failure of memory allocation, which allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed GIF file that specifies a large size.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0660 | None | None | Google Chrome before 4.0.249.78 sends an https URL in the Referer header of an http request in certain circumstances involving https to http redirection, which allows remote HTTP servers to obtain potentially sensitive information via standard HTTP logging.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0661 | None | None | WebCore/bindings/v8/custom/V8DOMWindowCustom.cpp in WebKit before r52401, as used in Google Chrome before 4.0.249.78, allows remote attackers to bypass the Same Origin Policy via vectors involving the window.open method.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0662 | None | None | The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not use the correct variables in calculations designed to prevent integer overflows, which allows attackers to leverage renderer access to cause a denial of service or possibly have unspecified other impact via bitmap data, related to deserialization. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0663 | None | None | The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not initialize the memory locations that will hold bitmap data, which might allow remote attackers to obtain potentially sensitive information from process memory by providing insufficient data, related to use of a (1) thumbnail database or (2) HTML canvas.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-0664 | None | None | Stack consumption vulnerability in the ChildProcessSecurityPolicy::CanRequestURL function in browser/child_process_security_policy.cc in Google Chrome before 4.0.249.78 allows remote attackers to cause a denial of service (memory consumption and application crash) via a URL that specifies multiple protocols, as demonstrated by a URL that begins with many repetitions of the view-source: substring. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1029 | None | None | Stack consumption vulnerability in the WebCore::CSSSelector function in WebKit, as used in Apple Safari 4.0.4, Apple Safari on iPhone OS and iPhone OS for iPod touch, and Google Chrome 4.0.249, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a STYLE element composed of a large number of *> sequences.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1228 | None | None | Multiple race conditions in the sandbox infrastructure in Google Chrome before 4.1.249.1036 have unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1229 | None | None | The sandbox infrastructure in Google Chrome before 4.1.249.1036 does not properly use pointers, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1230 | None | None | Google Chrome before 4.1.249.1036 does not have the expected behavior for attempts to delete Web SQL Databases and clear the Strict Transport Security (STS) state, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1231 | None | None | Google Chrome before 4.1.249.1036 processes HTTP headers before invoking the SafeBrowsing feature, which allows remote attackers to have an unspecified impact via crafted headers.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1232 | None | None | Google Chrome before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via a malformed SVG document.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1233 | None | None | Multiple integer overflows in Google Chrome before 4.1.249.1036 allow remote attackers to have an unspecified impact via vectors involving WebKit JavaScript objects.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1234 | None | None | Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to truncate the URL shown in the HTTP Basic Authentication dialog via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1235 | None | None | Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to trigger the omission of a download warning dialog via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1236 | None | None | The protocols function in platform/KURLGoogle.cpp in WebCore in WebKit before r55822, as used in Google Chrome before 4.1.249.1036 and Flock Browser 3.x before 3.0.0.4112, does not properly handle whitespace at the beginning of a URL, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted javascript: URL, as demonstrated by a \x00javascript:alert sequence. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1237 | None | None | Google Chrome 4.1 BETA before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via an empty SVG element.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1500 | None | None | Google Chrome before 4.1.249.1059 does not properly support forms, which has unknown impact and attack vectors, related to a "type confusion error."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1502 | None | None | Unspecified vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to access local files via vectors related to "developer tools."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1503 | None | None | Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://net-internals URI.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1504 | None | None | Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://downloads URI.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1505 | None | None | Google Chrome before 4.1.249.1059 does not prevent pages from loading with the New Tab page's privileges, which has unknown impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1506 | None | None | The Google V8 bindings in Google Chrome before 4.1.249.1059 allow attackers to cause a denial of service (memory corruption) via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1663 | None | None | The Google URL Parsing Library (aka google-url or GURL) in Google Chrome before 4.1.249.1064 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1664 | None | None | Google Chrome before 4.1.249.1064 does not properly handle HTML5 media, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1665 | None | None | Google Chrome before 4.1.249.1064 does not properly handle fonts, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1731 | None | None | Google Chrome on the HTC Hero allows remote attackers to cause a denial of service (application crash) via JavaScript that writes <marquee> sequences in an infinite loop.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1851 | None | None | Google Chrome, when the Invisible Hand extension is enabled, uses cookies during background HTTP requests in a possibly unexpected manner, which might allow remote web servers to identify specific persons and their product searches via HTTP request logging, related to a "cross-site data leakage" issue. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1992 | None | None | Google Chrome 1.0.154.48 executes a mail application in situations where an IFRAME element has a mailto: URL in its SRC attribute, which allows remote attackers to cause a denial of service (excessive application launches) via an HTML document with many IFRAME elements.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2105 | None | None | Google Chrome before 5.0.375.55 does not properly follow the Safe Browsing specification's requirements for canonicalization of URLs, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2106 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.55 might allow remote attackers to spoof the URL bar via vectors involving unload event handlers.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2107 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.55 allows attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the Safe Browsing functionality.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2108 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.55 allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2109 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.55 allows user-assisted remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the "drag + drop" functionality.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2110 | None | None | Google Chrome before 5.0.375.55 does not properly execute JavaScript code in the extension context, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2120 | None | None | Google Chrome 1.0.154.48 allows remote attackers to cause a denial of service (resource consumption) via JavaScript code containing an infinite loop that creates IFRAME elements for invalid news:// URIs.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1770 | None | None | WebKit in Apple Safari before 5.0 on Mac OS X 10.5 through 10.6 and Windows, Apple Safari before 4.1 on Mac OS X 10.4, and Google Chrome before 5.0.375.70 does not properly handle a transformation of a text node that has the IBM1147 character set, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document containing a BR element, related to a "type checking issue." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2295 | None | None | page/EventHandler.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 does not properly handle a change of the focused frame during the dispatching of keydown, which allows user-assisted remote attackers to redirect keystrokes via a crafted HTML document, aka rdar problem 7018610. NOTE: this might overlap CVE-2010-1422.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2296 | None | None | The implementation of unspecified DOM methods in Google Chrome before 5.0.375.70 allows remote attackers to bypass the Same Origin Policy via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2297 | None | None | rendering/FixedTableLayout.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an HTML document that has a large colspan attribute within a table.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2298 | None | None | browser/renderer_host/database_dispatcher_host.cc in Google Chrome before 5.0.375.70 on Linux does not properly handle ViewHostMsg_DatabaseOpenFile messages in chroot-based sandboxing, which allows remote attackers to bypass intended sandbox restrictions via vectors involving fchdir and chdir calls.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2299 | None | None | The Clipboard::DispatchObject function in app/clipboard/clipboard.cc in Google Chrome before 5.0.375.70 does not properly handle CBF_SMBITMAP objects in a ViewHostMsg_ClipboardWriteObjectsAsync message, which might allow remote attackers to execute arbitrary code via vectors involving crafted data from the renderer process, related to a "Type Confusion" issue.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2300 | None | None | Use-after-free vulnerability in the Element::normalizeAttributes function in dom/Element.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to handlers for DOM mutation events, aka rdar problem 7948784. NOTE: this might overlap CVE-2010-1759. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2301 | None | None | Cross-site scripting (XSS) vulnerability in editing/markup.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to inject arbitrary web script or HTML via vectors related to the node.innerHTML property of a TEXTAREA element. NOTE: this might overlap CVE-2010-1762.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2302 | None | None | Use-after-free vulnerability in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors involving remote fonts in conjunction with shadow DOM trees, aka rdar problem 8007953. NOTE: this might overlap CVE-2010-1771.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2645 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.99, when WebGL is used, allows remote attackers to cause a denial of service (out-of-bounds read) via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2646 | None | None | Google Chrome before 5.0.375.99 does not properly isolate sandboxed IFRAME elements, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2647 | None | None | Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an invalid SVG document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2648 | None | None | The implementation of the Unicode Bidirectional Algorithm (aka Bidi algorithm or UBA) in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2649 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (application crash) via an invalid image.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2650 | None | None | Unspecified vulnerability in Google Chrome before 5.0.375.99 has unknown impact and attack vectors, related to an "annoyance with print dialogs."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2651 | None | None | The Cascading Style Sheets (CSS) implementation in Google Chrome before 5.0.375.99 does not properly perform style rendering, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2652 | None | None | Google Chrome before 5.0.375.99 does not properly implement modal dialogs, which allows attackers to cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2897 | None | None | Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2898 | None | None | Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the GNU C Library, which has unknown impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2899 | None | None | Unspecified vulnerability in the layout implementation in Google Chrome before 5.0.375.125 allows remote attackers to obtain sensitive information from process memory via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2900 | None | None | Google Chrome before 5.0.375.125 does not properly handle a large canvas, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2901 | None | None | The rendering implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2902 | None | None | The SVG implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-2903 | None | None | Google Chrome before 5.0.375.125 performs unexpected truncation and improper eliding of hostnames, which has unspecified impact and remote attack vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3111 | None | None | Google Chrome before 6.0.472.53 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors, a different vulnerability than CVE-2010-2897.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3112 | None | None | Google Chrome before 5.0.375.127 does not properly implement file dialogs, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3113 | None | None | Google Chrome before 5.0.375.127, and webkitgtk before 1.2.5, does not properly handle SVG documents, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors related to state changes when using DeleteButtonController.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3114 | None | None | The text-editing implementation in Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not check a node type before performing a cast, which has unspecified impact and attack vectors related to (1) DeleteSelectionCommand.cpp, (2) InsertLineBreakCommand.cpp, or (3) InsertParagraphSeparatorCommand.cpp in WebCore/editing/.    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3115 | None | None | Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not properly implement the history feature, which might allow remote attackers to spoof the address bar via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3116 | None | None | Multiple use-after-free vulnerabilities in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to improper handling of MIME types by plug-ins. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3117 | None | None | Google Chrome before 5.0.375.127 does not properly implement the notifications feature, which allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3118 | None | None | The autosuggest feature in the Omnibox implementation in Google Chrome before 5.0.375.127 does not anticipate entry of passwords, which might allow remote attackers to obtain sensitive information by reading the network traffic generated by this feature.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3119 | None | None | Google Chrome before 5.0.375.127 and webkitgtk before 1.2.6 do not properly support the Ruby language, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3120 | None | None | Google Chrome before 5.0.375.127 does not properly implement the Geolocation feature, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3246 | None | None | Google Chrome before 6.0.472.53 does not properly handle the _blank value for the target attribute of unspecified elements, which allows remote attackers to bypass the pop-up blocker via unknown vectors.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3247 | None | None | Google Chrome before 6.0.472.53 does not properly restrict the characters in URLs, which allows remote attackers to spoof the appearance of the URL bar via homographic sequences.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3248 | None | None | Google Chrome before 6.0.472.53 does not properly restrict copying to the clipboard, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3249 | None | None | Google Chrome before 6.0.472.53 does not properly implement SVG filters, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "stale pointer" issue.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3250 | None | None | Unspecified vulnerability in Google Chrome before 6.0.472.53 allows remote attackers to enumerate the set of installed extensions via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3251 | None | None | The WebSockets implementation in Google Chrome before 6.0.472.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3252 | None | None | Use-after-free vulnerability in the Notifications presenter in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3253 | None | None | The implementation of notification permissions in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.                            |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3254 | None | None | The WebSockets implementation in Google Chrome before 6.0.472.53 does not properly handle integer values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3255 | None | None | Google Chrome before 6.0.472.53 and webkitgtk before 1.2.6 do not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3256 | None | None | Google Chrome before 6.0.472.53 does not properly limit the number of stored autocomplete entries, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3257 | None | None | Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving element focus.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3258 | None | None | The sandbox implementation in Google Chrome before 6.0.472.53 does not properly deserialize parameters, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3259 | None | None | WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, does not properly restrict read access to images derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive image data via a crafted web site. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3411 | None | None | Google Chrome before 6.0.472.59 on Linux does not properly handle cursors, which might allow attackers to cause a denial of service (assertion failure) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3412 | None | None | Race condition in the console implementation in Google Chrome before 6.0.472.59 has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3413 | None | None | Unspecified vulnerability in the pop-up blocking functionality in Google Chrome before 6.0.472.59 allows remote attackers to cause a denial of service (application crash) via unknown vectors.   |

|               |                    |               |          |      |  |
|---------------|--------------------|---------------|----------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3414 | None     | None | Google Chrome before 6.0.472.59 on Mac OS X does not properly implement file dialogs, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. NOTE: this issue exists because of an incorrect fix for CVE-2010-3112 on Mac OS X.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3415 | None     | None | Google Chrome before 6.0.472.59 does not properly implement Geolocation, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3416 | CRITICAL | 9.8  | Google Chrome before 6.0.472.59 on Linux does not properly implement the Khmer locale, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3417 | None     | None | Google Chrome before 6.0.472.59 does not prompt the user before granting access to the extension history, which allows attackers to obtain potentially sensitive information via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1767 | None     | None | Cross-site request forgery (CSRF) vulnerability in loader/DocumentThreadableLoader.cpp in WebCore in WebKit before r57041, as used in Google Chrome before 4.1.249.1059, allows remote attackers to hijack the authentication of unspecified victims via a crafted synchronous preflight XMLHttpRequest operation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1772 | HIGH     | 8.8  | Use-after-free vulnerability in page/Geolocation.cpp in WebCore in WebKit before r59859, as used in Google Chrome before 5.0.375.70, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted web site, related to failure to stop timers associated with geolocation upon deletion of a document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1773 | HIGH     | 8.8  | Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp in WebCore in WebKit before r59950, as used in Google Chrome before 5.0.375.70, allows remote attackers to obtain sensitive information, cause a denial of service (memory corruption and application crash), or possibly execute arbitrary code via vectors related to list markers for HTML lists, aka rdar problem 8009118. |

|               |                    |               |          |      |   |
|---------------|--------------------|---------------|----------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1823 | None     | None | Use-after-free vulnerability in WebKit before r65958, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger use of document APIs such as document.close during parsing, as demonstrated by a Cascading Style Sheets (CSS) file referencing an invalid SVG font, aka rdar problem 8442098. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1824 | None     | None | Use-after-free vulnerability in WebKit, as used in Apple iTunes before 10.2 on Windows, Apple Safari, and Google Chrome before 6.0.472.59, allows remote attackers to execute arbitrary code or cause a denial of service via vectors related to SVG styles, the DOM tree, and error messages.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1825 | None     | None | Use-after-free vulnerability in WebKit, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to nested SVG elements.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-1822 | HIGH     | 8.8  | WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3 and Google Chrome before 6.0.472.62, does not properly perform a cast of an unspecified variable, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an SVG element in a non-SVG document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3729 | CRITICAL | 9.8  | The SPDY protocol implementation in Google Chrome before 6.0.472.62 does not properly manage buffers, which might allow remote attackers to execute arbitrary code via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-3730 | HIGH     | 8.8  | Google Chrome before 6.0.472.62 does not properly use information about the origin of a document to manage properties, which allows remote attackers to have an unspecified impact via a crafted web site, related to a "property pollution" issue.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4033 | None     | None | Google Chrome before 7.0.517.41 does not properly implement the autofill and autocomplete functionality, which allows remote attackers to conduct "profile spamming" attacks via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4034 | None     | None | Google Chrome before 7.0.517.41 does not properly handle forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.   |

|               |                    |               |          |      |  |
|---------------|--------------------|---------------|----------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4035 | None     | None | Google Chrome before 7.0.517.41 does not properly perform autofill operations for forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4036 | None     | None | Google Chrome before 7.0.517.41 does not properly handle the unloading of a page, which allows remote attackers to spoof URLs via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4037 | None     | None | Unspecified vulnerability in Google Chrome before 7.0.517.41 allows remote attackers to bypass the pop-up blocker via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4038 | HIGH     | 7.5  | The Web Sockets implementation in Google Chrome before 7.0.517.41 does not properly handle a shutdown action, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4039 | CRITICAL | 9.8  | Google Chrome before 7.0.517.41 on Linux does not properly set the PATH environment variable, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4040 | HIGH     | 7.8  | Google Chrome before 7.0.517.41 does not properly handle animated GIF images, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4041 | CRITICAL | 9.8  | The sandbox implementation in Google Chrome before 7.0.517.41 on Linux does not properly constrain worker processes, which might allow remote attackers to bypass intended access restrictions via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4042 | CRITICAL | 9.8  | Google Chrome before 7.0.517.41 does not properly handle element maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "stale elements."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4197 | CRITICAL | 9.8  | Use-after-free vulnerability in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text editing.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4198 | HIGH     | 8.8  | WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, does not properly handle large text areas, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted HTML document. |

|               |                    |               |          |      |   |
|---------------|--------------------|---------------|----------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4199 | HIGH     | 8.8  | Google Chrome before 7.0.517.44 does not properly perform a cast of an unspecified variable during processing of an SVG use element, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SVG document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4201 | CRITICAL | 9.8  | Use-after-free vulnerability in Google Chrome before 7.0.517.44 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text control selections.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4202 | CRITICAL | 9.8  | Multiple integer overflows in Google Chrome before 7.0.517.44 on Linux allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4203 | CRITICAL | 9.8  | WebM libvpx (aka the VP8 Codec SDK) before 0.9.5, as used in Google Chrome before 7.0.517.44, allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via invalid frames.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4204 | CRITICAL | 9.8  | WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, accesses a frame object after this object has been destroyed, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4205 | CRITICAL | 9.8  | Google Chrome before 7.0.517.44 does not properly handle the data types of event objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4206 | HIGH     | 8.8  | Array index error in the FEBlend::apply function in WebCore/platform/graphics/filters/FEBlend.cpp in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted SVG document, related to effects in the application of filters. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4008 | None     | None | libxml2 before 2.7.8, as used in Google Chrome before 7.0.517.44, Apple Safari 5.0.2 and earlier, and other products, reads from invalid memory locations during processing of malformed XPath expressions, which allows context-dependent attackers to cause a denial of service (application crash) via a crafted XML document.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4482 | None | None | Unspecified vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to bypass the pop-up blocker via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4483 | None | None | Google Chrome before 8.0.552.215 does not properly restrict read access to videos derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive video data via a crafted web site. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4484 | None | None | Google Chrome before 8.0.552.215 does not properly handle HTML5 databases, which allows attackers to cause a denial of service (application crash) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4485 | None | None | Google Chrome before 8.0.552.215 does not properly restrict the generation of file dialogs, which allows remote attackers to cause a denial of service (reduced usability and possible application crash) via a crafted web site.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4486 | None | None | Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to history handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4487 | None | None | Incomplete blacklist vulnerability in Google Chrome before 8.0.552.215 on Linux and Mac OS X allows remote attackers to have an unspecified impact via a "dangerous file."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4488 | None | None | Google Chrome before 8.0.552.215 does not properly handle HTTP proxy authentication, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4489 | None | None | libvpx, as used in Google Chrome before 8.0.552.215 and possibly other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebM video. NOTE: this vulnerability exists because of a regression.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4490 | None | None | Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via malformed video content that triggers an indexing error.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4491 | None | None | Google Chrome before 8.0.552.215 does not properly restrict privileged extensions, which allows remote attackers to cause a denial of service (memory corruption) via a crafted extension.   |

|               |                    |               |                  |            |   |
|---------------|--------------------|---------------|------------------|------------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4492 | None             | None       | Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animations.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4493 | None             | None       | Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service via vectors related to the handling of mouse dragging events.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4494 | None             | None       | Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4574 | None             | None       | The Pickle::Pickle function in base/pickle.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 on 64-bit Linux platforms does not properly perform pointer arithmetic, which allows remote attackers to bypass message deserialization validation, and cause a denial of service or possibly have unspecified other impact, via invalid pickle data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4575 | None             | None       | The ThemeInstalledInfoBarDelegate::Observe function in browser/extensions/theme_installed_infobar_delegate.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle incorrect tab interaction by an extension, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4576 | None             | None       | browser/worker_host/message_port_dispatcher.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle certain postMessage calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code that creates a web worker.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4577 | ['HIGH', 'HIGH'] | [7.5, 7.5] | The CSSParser::parseFontFaceSrc function in WebCore/css/CSSParser.cpp in WebKit, as used in Google Chrome before 8.0.552.224, Chrome OS before 8.0.552.343, webkitgtk before 1.2.6, and other products does not properly parse Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted local font, related to "Type Confusion." |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-4578 | None | None | Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 do not properly perform cursor handling, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0470 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle extensions notification, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0471 | None | None | The node-iteration implementation in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 does not properly handle pointers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0472 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle the printing of PDF documents, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a multi-page document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0473 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with CANVAS elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0474 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0475 | None | None | Use-after-free vulnerability in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a PDF document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0476 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allow remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a PDF document that triggers an out-of-memory error.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0477 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle a mismatch in video frame sizes, which allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0478 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle SVG use elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0479 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly interact with extensions, which allows remote attackers to cause a denial of service via a crafted extension that triggers an uninitialized pointer.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0480 | None | None | Multiple buffer overflows in vorbis_dec.c in the Vorbis decoder in FFmpeg, as used in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a crafted WebM file, related to buffers for (1) the channel floor and (2) the channel residue. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0481 | None | None | Buffer overflow in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF shading.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0482 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of anchors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0483 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of video, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0484 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform DOM node removal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale rendering node."   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0485 | None | None | Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle speech data, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "stale pointer."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0776 | None | None | The sandbox implementation in Google Chrome before 9.0.597.84 on Mac OS X might allow remote attackers to obtain potentially sensitive information about local files via vectors related to the stat system call.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0777 | None | None | Use-after-free vulnerability in Google Chrome before 9.0.597.84 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to image loading.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0778 | None | None | Google Chrome before 9.0.597.84 does not properly restrict drag and drop operations, which might allow remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0779 | None | None | Google Chrome before 9.0.597.84 does not properly handle a missing key in an extension, which allows remote attackers to cause a denial of service (application crash) via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0780 | None | None | The PDF event handler in Google Chrome before 9.0.597.84 does not properly interact with print operations, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0781 | None | None | Google Chrome before 9.0.597.84 does not properly handle autofill profile merging, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0782 | None | None | Google Chrome before 9.0.597.84 on Mac OS X does not properly mitigate an unspecified flaw in the Mac OS X 10.5 SSL libraries, which allows remote attackers to cause a denial of service (application crash) via unknown vectors.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0783 | None | None | Unspecified vulnerability in Google Chrome before 9.0.597.84 allows user-assisted remote attackers to cause a denial of service (application crash) via vectors involving a "bad volume setting."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0784 | None | None | Race condition in Google Chrome before 9.0.597.84 allows remote attackers to execute arbitrary code via vectors related to audio.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0981 | None | None | Google Chrome before 9.0.597.94 does not properly perform event handling for animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0982 | None | None | Use-after-free vulnerability in Google Chrome before 9.0.597.94 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG font faces.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0983 | None | None | Google Chrome before 9.0.597.94 does not properly handle anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0984 | None | None | Google Chrome before 9.0.597.94 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-0985 | None | None | Google Chrome before 9.0.597.94 does not properly perform process termination upon memory exhaustion, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1042 | None | None | Use-after-free vulnerability in flimflamd in flimflam in Google Chrome OS before 0.9.130.14 Beta allows user-assisted remote attackers to cause a denial of service (daemon crash) by providing the name of a hidden WiFi network that does not respond to connection attempts.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1059 | None | None | Use-after-free vulnerability in WebCore in WebKit before r77705, as used in Google Chrome before 11.0.672.2 and other products, allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that entice a user to resubmit a form, related to improper handling of provisional items by the HistoryController component, aka rdar problem 8938557. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1107 | None | None | Unspecified vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to spoof the URL bar via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1108 | None | None | Google Chrome before 9.0.597.107 does not properly implement JavaScript dialogs, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1109 | None | None | Google Chrome before 9.0.597.107 does not properly process nodes in Cascading Style Sheets (CSS) stylesheets, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1110 | None | None | Google Chrome before 9.0.597.107 does not properly implement key frame rules, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1111 | None | None | Google Chrome before 9.0.597.107 does not properly implement forms controls, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1112 | None | None | Google Chrome before 9.0.597.107 does not properly perform SVG rendering, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1113 | None | None | Google Chrome before 9.0.597.107 on 64-bit Linux platforms does not properly perform pickle deserialization, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1114 | None | None | Google Chrome before 9.0.597.107 does not properly handle tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1115 | None | None | Google Chrome before 9.0.597.107 does not properly render tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1116 | None | None | Google Chrome before 9.0.597.107 does not properly handle SVG animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1117 | None | None | Google Chrome before 9.0.597.107 does not properly handle XHTML documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale nodes."  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1118 | None | None | Google Chrome before 9.0.597.107 does not properly handle TEXTAREA elements, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1119 | None | None | Google Chrome before 9.0.597.107 does not properly determine device orientation, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1120 | None | None | The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71717.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1121 | None | None | Integer overflow in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a TEXTAREA element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1122 | None | None | The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71960.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1123 | None | None | Google Chrome before 9.0.597.107 does not properly restrict access to internal extension functions, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1124 | None | None | Use-after-free vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to blocked plug-ins.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1125 | None | None | Google Chrome before 9.0.597.107 does not properly perform layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1306 | None | None | Unspecified vulnerability in the Scratchpad application in Google Chrome OS before R10 0.10.156.46 Beta has unknown impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1185 | None | None | Google Chrome before 10.0.648.127 does not prevent (1) navigation and (2) close operations on the top location of a sandboxed frame, which has unspecified impact and remote attack vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1186 | None | None | Google Chrome before 10.0.648.127 on Linux does not properly handle parallel execution of calls to the print method, which might allow remote attackers to cause a denial of service (application crash) via crafted JavaScript code. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1187 | None | None | Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1188 | None | None | Google Chrome before 10.0.648.127 does not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1189 | None | None | Google Chrome before 10.0.648.127 does not properly perform box layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1190 | None | None | The Web Workers implementation in Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1191 | None | None | Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of DOM URLs.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1192 | None | None | Google Chrome before 10.0.648.127 on Linux does not properly handle Unicode ranges, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1193 | None | None | Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1194 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 10.0.648.127 allow remote attackers to bypass the pop-up blocker via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1195 | None | None | Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "document script lifetime handling."          |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1196 | None | None | The OGG container implementation in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1197 | None | None | Google Chrome before 10.0.648.127 does not properly perform table painting, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1198 | None | None | The video functionality in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger use of a malformed "out-of-bounds structure."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1199 | None | None | Google Chrome before 10.0.648.127 does not properly handle DataView objects, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1200 | None | None | Google Chrome before 10.0.648.127 does not properly perform a cast of an unspecified variable during text rendering, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1201 | None | None | The context implementation in WebKit, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1202 | None | None | The xsltGenerateIdFunction function in functions.c in libxslt 1.1.26 and earlier, as used in Google Chrome before 10.0.648.127 and other products, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1203 | None | None | Google Chrome before 10.0.648.127 does not properly handle SVG cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1204 | None | None | Google Chrome before 10.0.648.127 does not properly handle attributes, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via a crafted document.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1285 | None | None | The regular-expression functionality in Google Chrome before 10.0.648.127 does not properly implement reentrancy, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1286 | None | None | Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger incorrect access to memory.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1413 | None | None | Google Chrome before 10.0.648.127 on Linux does not properly mitigate an unspecified flaw in an X server, which allows remote attackers to cause a denial of service (application crash) via vectors involving long messages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1290 | None | None | Integer overflow in WebKit, as used on the Research In Motion (RIM) BlackBerry Torch 9800 with firmware 6.0.0.246, in Google Chrome before 10.0.648.133, and in Apple Safari before 5.0.5, allows remote attackers to execute arbitrary code via unknown vectors related to CSS "style handling," nodesets, and a length value, as demonstrated by Vincenzo Iozzo, Willem Pinckaers, and Ralf-Philipp Weinmann during a Pwn2Own competition at CanSecWest 2011. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1465 | None | None | The SPDY implementation in net/http/http_network_transaction.cc in Google Chrome before 11.0.696.14 drains the bodies from SPDY responses, which might allow remote SPDY servers to cause a denial of service (application exit) by canceling a stream.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1291 | None | None | Google Chrome before 10.0.648.204 does not properly handle base strings, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "buffer error."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1292 | None | None | Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1293 | None | None | Use-after-free vulnerability in the HTMLCollection implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1294 | None | None | Google Chrome before 10.0.648.204 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1295 | None | None | WebKit, as used in Google Chrome before 10.0.648.204 and Apple Safari before 5.0.6, does not properly handle node parentage, which allows remote attackers to cause a denial of service (DOM tree corruption), conduct cross-site scripting (XSS) attacks, or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1296 | None | None | Google Chrome before 10.0.648.204 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1071 | None | None | The GNU C Library (aka glibc or libc6) before 2.12.2 and Embedded GLIBC (EGLIBC) allow context-dependent attackers to execute arbitrary code or cause a denial of service (memory consumption) via a long UTF8 string that is used in an fnmatch call, aka a "stack extension attack," a related issue to CVE-2010-2898, CVE-2010-1917, and CVE-2007-4782, as originally reported for use of this library by Google Chrome.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1691 | None | None | The counterToCSSValue function in CSSComputedStyleDeclaration.cpp in the Cascading Style Sheets (CSS) implementation in WebCore in WebKit before r82222, as used in Google Chrome before 11.0.696.43 and other products, does not properly handle access to the (1) counterIncrement and (2) counterReset attributes of CSSStyleDeclaration data provided by a getComputedStyle method call, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1300 | None | None | The Program::getActiveUniformMaxLength function in libGLSv2/Program.cpp in libGLSv2.dll in the WebGLSv2 library in Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox 4.x before 4.0.1 on Windows and in the GPU process in Google Chrome before 10.0.648.205 on Windows, allows remote attackers to execute arbitrary code via unspecified vectors, related to an "off-by-three" error.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1301 | None | None | Use-after-free vulnerability in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1302 | None | None | Heap-based buffer overflow in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1303 | None | None | Google Chrome before 11.0.696.57 does not properly handle floating objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1304 | None | None | Unspecified vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to bypass the pop-up blocker via vectors related to plug-ins.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1305 | None | None | Race condition in Google Chrome before 11.0.696.57 on Linux and Mac OS X allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to linked lists and a database.          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1434 | None | None | Google Chrome before 11.0.696.57 does not ensure thread safety during handling of MIME data, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1435 | None | None | Google Chrome before 11.0.696.57 does not properly implement the tabs permission for extensions, which allows remote attackers to read local files via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1436 | None | None | Google Chrome before 11.0.696.57 on Linux does not properly interact with the X Window System, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1437 | None | None | Multiple integer overflows in Google Chrome before 11.0.696.57 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float rendering.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1438 | None | None | Google Chrome before 11.0.696.57 allows remote attackers to bypass the Same Origin Policy via vectors involving blobs.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1439 | None | None | Google Chrome before 11.0.696.57 on Linux does not properly isolate renderer processes, which has unspecified impact and remote attack vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1440 | None | None | Use-after-free vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the ruby element and Cascading Style Sheets (CSS) token sequences.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1441 | None | None | Google Chrome before 11.0.696.57 does not properly perform a cast of an unspecified variable during handling of floating select lists, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1442 | None | None | Google Chrome before 11.0.696.57 does not properly handle mutation events, which allows remote attackers to cause a denial of service (node tree corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1443 | None | None | Google Chrome before 11.0.696.57 does not properly implement layering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."                                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1444 | None | None | Race condition in the sandbox launcher implementation in Google Chrome before 11.0.696.57 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1445 | None | None | Google Chrome before 11.0.696.57 does not properly handle SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1446 | None | None | Google Chrome before 11.0.696.57 allows remote attackers to spoof the URL bar via vectors involving (1) a navigation error or (2) an interrupted load.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1447 | None | None | Google Chrome before 11.0.696.57 does not properly handle drop-down lists, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1448 | None | None | Google Chrome before 11.0.696.57 does not properly perform height calculations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."                             |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1449 | None | None | Use-after-free vulnerability in the WebSockets implementation in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1450 | None | None | Google Chrome before 11.0.696.57 does not properly present file dialogs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1451 | None | None | Google Chrome before 11.0.696.57 does not properly handle DOM id maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1452 | None | None | Google Chrome before 11.0.696.57 allows user-assisted remote attackers to spoof the URL bar via vectors involving a redirect and a manual reload.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1454 | None | None | Use-after-free vulnerability in the DOM id handling functionality in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1455 | None | None | Google Chrome before 11.0.696.57 does not properly handle PDF documents with multipart encoding, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1456 | None | None | Google Chrome before 11.0.696.57 does not properly handle PDF forms, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2075 | None | None | Unspecified vulnerability in Google Chrome 11.0.696.65 on Windows 7 SP1 allows remote attackers to execute arbitrary code via unknown vectors. NOTE: as of 20110510, the only disclosure is a vague advisory that possibly relates to multiple vulnerabilities or multiple products. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1799 | None | None | Google Chrome before 11.0.696.68 does not properly perform casts of variables during interaction with the WebKit engine, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1800 | None | None | Multiple integer overflows in the SVG Filters implementation in WebCore in WebKit in Google Chrome before 11.0.696.68 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2162 | None | None | Multiple unspecified vulnerabilities in FFmpeg 0.4.x through 0.6.x, as used in MPlayer 1.0 and other products, in Mandriva Linux 2009.0, 2010.0, and 2010.1; Corporate Server 4.0 (aka CS4.0); and Mandriva Enterprise Server 5 (aka MES5) have unknown impact and attack vectors, related to issues "originally discovered by Google Chrome developers." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2169 | None | None | Google Chrome OS before R12 0.12.433.38 Beta allows local users to gain privileges by creating a /var/lib/chromeos-aliases.conf file and placing commands in it.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2170 | None | None | Google Chrome OS before R12 0.12.433.38 Beta, when Guest mode is enabled, does not prevent changes on the about:flags page, which has unspecified impact and local attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2171 | None | None | Unspecified vulnerability in the dbugs package in Google Chrome OS before R12 0.12.433.38 Beta has unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1801 | None | None | Unspecified vulnerability in Google Chrome before 11.0.696.71 allows remote attackers to bypass the pop-up blocker via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1804 | None | None | rendering/RenderBox.cpp in WebCore in WebKit before r86862, as used in Google Chrome before 11.0.696.71, does not properly render floats, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1806 | None | None | Google Chrome before 11.0.696.71 does not properly implement the GPU command buffer, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1807 | None | None | Google Chrome before 11.0.696.71 does not properly handle blobs, which allows remote attackers to execute arbitrary code via unspecified vectors that trigger an out-of-bounds write.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1808 | None | None | Use-after-free vulnerability in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to incorrect integer calculations during float handling.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1809 | None | None | Use-after-free vulnerability in the accessibility feature in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1810 | None | None | The Cascading Style Sheets (CSS) implementation in Google Chrome before 12.0.742.91 does not properly restrict access to the visit history, which allows remote attackers to obtain sensitive information via unspecified vectors.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1811 | None | None | Google Chrome before 12.0.742.91 does not properly handle a large number of form submissions, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1812 | None | None | Google Chrome before 12.0.742.91 allows remote attackers to bypass intended access restrictions via vectors related to extensions.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1813 | None | None | Google Chrome before 12.0.742.91 does not properly implement the framework for extensions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1814 | None | None | Google Chrome before 12.0.742.91 attempts to read data from an uninitialized pointer, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1815 | None | None | Google Chrome before 12.0.742.91 allows remote attackers to inject script into a tab page via vectors related to extensions.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1816 | None | None | Use-after-free vulnerability in the developer tools in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1817 | None | None | Google Chrome before 12.0.742.91 does not properly implement history deletion, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.                        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1818 | None | None | Use-after-free vulnerability in the image loader in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1819 | None | None | Google Chrome before 12.0.742.91 allows remote attackers to perform unspecified injection into a chrome:// page via vectors related to extensions.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2332 | None | None | Google V8, as used in Google Chrome before 12.0.742.91, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2342 | None | None | The DOM implementation in Google Chrome before 12.0.742.91 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2345 | None | None | The NPAPI implementation in Google Chrome before 12.0.742.112 does not properly handle strings, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2346 | None | None | Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG fonts.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2347 | None | None | Google Chrome before 12.0.742.112 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2348 | None | None | Google V8, as used in Google Chrome before 12.0.742.112, performs an incorrect bounds check, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2349 | None | None | Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text selection.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2350 | None | None | The HTML parser in Google Chrome before 12.0.742.112 does not properly address "lifetime and re-entrancy issues," which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2351 | None | None | Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2599 | None | None | Google Chrome 11 does not block use of a cross-domain image as a WebGL texture, which allows remote attackers to obtain approximate copies of arbitrary images via a timing attack involving a crafted WebGL fragment shader.                          |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2600 | None | None | The GPU support functionality in Windows XP does not properly restrict rendering time, which allows remote attackers to cause a denial of service (system crash) via vectors involving WebGL and (1) shader programs or (2) complex 3D geometry, as demonstrated by using Mozilla Firefox or Google Chrome to visit the lots-of-polys-example.html test page in the Khronos WebGL SDK. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2601 | None | None | The GPU support functionality in Mac OS X does not properly restrict rendering time, which allows remote attackers to cause a denial of service (desktop hang) via vectors involving WebGL and (1) shader programs or (2) complex 3D geometry, as demonstrated by using Mozilla Firefox or Google Chrome to visit the lots-of-polys-example.html test page in the Khronos WebGL SDK.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2602 | None | None | The NVIDIA Geforce 310 driver 6.14.12.7061 on Windows XP SP3 allows remote attackers to cause a denial of service (system crash) via a crafted web page that is visited with Google Chrome or Mozilla Firefox, as demonstrated by the lots-of-polys-example.html test page in the Khronos WebGL SDK.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2603 | None | None | The NVIDIA 9400M driver 6.2.6 on Mac OS X 10.6.7 allows remote attackers to cause a denial of service (desktop hang) via a crafted web page that is visited with Google Chrome or Mozilla Firefox, as demonstrated by the lots-of-polys-example.html test page in the Khronos WebGL SDK.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2604 | None | None | The Intel G41 driver 6.14.10.5355 on Windows XP SP3 allows remote attackers to cause a denial of service (system crash) via a crafted web page that is visited with Google Chrome or Mozilla Firefox, as demonstrated by the lots-of-polys-example.html test page in the Khronos WebGL SDK.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2761 | None | None | Google Chrome 14.0.794.0 does not properly handle a reload of a page generated in response to a POST, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted web site, related to GetWidget methods.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2358 | None | None | Google Chrome before 13.0.782.107 does not ensure that extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2359 | None | None | Google Chrome before 13.0.782.107 does not properly track line boxes during rendering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2360 | None | None | Google Chrome before 13.0.782.107 does not ensure that the user is prompted before download of a dangerous file, which makes it easier for remote attackers to bypass intended content restrictions via a crafted web site.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2361 | None | None | The Basic Authentication dialog implementation in Google Chrome before 13.0.782.107 does not properly handle strings, which might make it easier for remote attackers to capture credentials via a crafted web site.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2782 | None | None | The drag-and-drop implementation in Google Chrome before 13.0.782.107 on Linux does not properly enforce permissions for files, which allows user-assisted remote attackers to bypass intended access restrictions via unspecified vectors.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2783 | None | None | Google Chrome before 13.0.782.107 does not ensure that developer-mode NPAPI extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2784 | None | None | Google Chrome before 13.0.782.107 allows remote attackers to obtain sensitive information via a request for the GL program log, which reveals a local path in an unspecified log entry.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2785 | None | None | The extensions implementation in Google Chrome before 13.0.782.107 does not properly validate the URL for the home page, which allows remote attackers to have an unspecified impact via a crafted extension.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2786 | None | None | Google Chrome before 13.0.782.107 does not ensure that the speech-input bubble is shown on the product's screen, which might make it easier for remote attackers to make audio recordings via a crafted web page containing an INPUT element.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2787 | None | None | Google Chrome before 13.0.782.107 does not properly address re-entrancy issues associated with the GPU lock, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.                                  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2788 | None | None | Buffer overflow in the inspector serialization functionality in Google Chrome before 13.0.782.107 allows user-assisted remote attackers to have an unspecified impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2789 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to instantiation of the Pepper plug-in.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2790 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving floating styles.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2791 | None | None | The International Components for Unicode (ICU) functionality in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2792 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float removal.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2793 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media selectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2794 | None | None | Google Chrome before 13.0.782.107 does not properly perform text iteration, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2795 | None | None | Google Chrome before 13.0.782.107 does not prevent calls to functions in other frames, which allows remote attackers to bypass intended access restrictions via a crafted web site, related to a "cross-frame function leak."                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2796 | None | None | Use-after-free vulnerability in Skia, as used in Google Chrome before 13.0.782.107, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2797 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to resource caching.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2798 | None | None | Google Chrome before 13.0.782.107 does not properly restrict access to internal schemes, which allows remote attackers to have an unspecified impact via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2799 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to HTML range handling.                                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2800 | None | None | Google Chrome before 13.0.782.107 allows remote attackers to obtain potentially sensitive information about client-side redirect targets via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2801 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the frame loader.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2802 | None | None | Google V8, as used in Google Chrome before 13.0.782.107, does not properly perform const lookups, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted web site. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2803 | None | None | Google Chrome before 13.0.782.107 does not properly handle Skia paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2804 | None | None | Google Chrome before 13.0.782.107 does not properly handle nested functions in PDF documents, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted document.     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2805 | None | None | Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy and conduct script injection attacks via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2818 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to display box rendering.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2819 | None | None | Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy via vectors related to handling of the base URI.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2008-7294 | None | None | Google Chrome before 4.0.211.0 cannot properly restrict modifications to cookies established in HTTPS sessions, which allows man-in-the-middle attackers to overwrite or delete arbitrary cookies via a Set-Cookie header in an HTTP response, related to lack of the HTTP Strict Transport Security (HSTS) includeSubDomains feature, aka a "cookie forcing" issue. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2806 | None | None | Google Chrome before 13.0.782.215 on Windows does not properly handle vertex data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2821 | None | None | Double free vulnerability in libxml2, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted XPath expression.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2822 | None | None | Google Chrome before 13.0.782.215 on Windows does not properly parse URLs located on the command line, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2823 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a line box.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2824 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2825 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving custom fonts.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2826 | None | None | Google Chrome before 13.0.782.215 allows remote attackers to bypass the Same Origin Policy via vectors related to empty origins.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2827 | None | None | Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text searching.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2828 | None | None | Google V8, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2829 | None | None | Integer overflow in Google Chrome before 13.0.782.215 on 32-bit platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving uniform arrays.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2839 | None | None | The PDF implementation in Google Chrome before 13.0.782.215 on Linux does not properly use the memset library function, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3389 | None | None | The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3420 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 14.0.835.157 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3421 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 14.0.835.125 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2834 | None | None | Double free vulnerability in libxml2, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2835 | None | None | Race condition in Google Chrome before 14.0.835.163 allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the certificate cache.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2836 | None | None | Google Chrome before 14.0.835.163 does not require Infobar interaction before use of the Windows Media Player plug-in, which makes it easier for remote attackers to have an unspecified impact via crafted Flash content.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2837 | None | None | Google Chrome before 14.0.835.163 on Linux does not use the PIC and PIE compiler options for position-independent code, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2838 | None | None | Google Chrome before 14.0.835.163 does not properly consider the MIME type during the loading of a plug-in, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2840 | None | None | Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to "unusual user interaction."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2841 | None | None | Google Chrome before 14.0.835.163 does not properly perform garbage collection during the processing of PDF documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2842 | None | None | The installer in Google Chrome before 14.0.835.163 on Mac OS X does not properly handle lock files, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2843 | None | None | Google Chrome before 14.0.835.163 does not properly handle media buffers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2844 | None | None | Google Chrome before 14.0.835.163 does not properly process MP3 files, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2846 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unload event handling.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2847 | None | None | Use-after-free vulnerability in the document loader in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2848 | None | None | Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to the forward button.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2849 | None | None | The WebSockets implementation in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2850 | None | None | Google Chrome before 14.0.835.163 does not properly handle Khmer characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2851 | None | None | Google Chrome before 14.0.835.163 does not properly handle video, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2852 | None | None | Off-by-one error in Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2853 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2854 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "ruby / table style handling."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2855 | None | None | Google Chrome before 14.0.835.163 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2856 | None | None | Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2857 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the focus controller.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2858 | None | None | Google Chrome before 14.0.835.163 does not properly handle triangle arrays, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2859 | None | None | Google Chrome before 14.0.835.163 uses incorrect permissions for non-gallery pages, which has unspecified impact and attack vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2860 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to table styles.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2861 | None | None | Google Chrome before 14.0.835.163 does not properly handle strings in PDF documents, which allows remote attackers to have an unspecified impact via a crafted document that triggers an incorrect read operation.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2862 | None | None | Google V8, as used in Google Chrome before 14.0.835.163, does not properly restrict access to built-in objects, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2864 | None | None | Google Chrome before 14.0.835.163 does not properly handle Tibetan characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2874 | None | None | Google Chrome before 14.0.835.163 does not perform an expected pin operation for a self-signed certificate during a session, which has unspecified impact and remote attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2875 | None | None | Google V8, as used in Google Chrome before 14.0.835.163, does not properly perform object sealing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3234 | None | None | Google Chrome before 14.0.835.163 does not properly handle boxes, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2876 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a text line box.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2877 | None | None | Google Chrome before 14.0.835.202 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale font."                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2878 | None | None | Google Chrome before 14.0.835.202 does not properly restrict access to the window prototype, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2879 | None | None | Google Chrome before 14.0.835.202 does not properly consider object lifetimes and thread safety during the handling of audio nodes, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2880 | None | None | Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2881 | None | None | Google Chrome before 14.0.835.202 does not properly handle Google V8 hidden objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3873 | None | None | Google Chrome before 14.0.835.202 does not properly implement shader translation, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2845 | None | None | Google Chrome before 15.0.874.102 does not properly handle history data, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3875 | None | None | Google Chrome before 15.0.874.102 does not properly handle drag and drop operations on URL strings, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3876 | None | None | Google Chrome before 15.0.874.102 does not properly handle downloading files that have whitespace characters at the end of a filename, which has unspecified impact and user-assisted remote attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3877 | None | None | Cross-site scripting (XSS) vulnerability in the appcache internals page in Google Chrome before 15.0.874.102 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3878 | None | None | Race condition in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker process initialization.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3879 | None | None | Google Chrome before 15.0.874.102 does not prevent redirects to chrome: URLs, which has unspecified impact and remote attack vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3880 | None | None | Google Chrome before 15.0.874.102 does not prevent use of an unspecified special character as a delimiter in HTTP headers, which has unknown impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3881 | None | None | WebKit, as used in Google Chrome before 15.0.874.102 and Android before 4.4, allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks via vectors related to (1) the DOMWindow::clear function and use of a selection object, (2) the Object::GetRealNamedPropertyInPrototypeChain function and use of an __proto__ property, (3) the HTMLPlugInImageElement::allowedToLoadFrameURL function and use of a javascript: URL, (4) incorrect origins for XSLT-generated documents in the XSLTProcessor::createDocumentFromSource function, and (5) improper handling of synchronous frame loads in the ScriptController::executelfJavaScriptURL function. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3882 | None | None | Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media buffers.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3883 | None | None | Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counters.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3884 | None | None | Google Chrome before 15.0.874.102 does not properly address timing issues during DOM traversal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3885 | None | None | Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to stale Cascading Style Sheets (CSS) token-sequence data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3886 | None | None | Google V8, as used in Google Chrome before 15.0.874.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers out-of-bounds write operations.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3887 | None | None | Google Chrome before 15.0.874.102 does not properly handle javascript: URLs, which allows remote attackers to bypass intended access restrictions and read cookies via unspecified vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3888 | None | None | Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing operations in conjunction with an unknown plug-in.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3889 | None | None | Heap-based buffer overflow in the Web Audio implementation in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3890 | None | None | Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video source handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3891 | None | None | Google Chrome before 15.0.874.102 does not properly restrict access to internal Google V8 functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2830 | None | None | Google V8, as used in Google Chrome before 14.0.835.163, does not properly implement script object wrappers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3640 | None | None | Untrusted search path vulnerability in Mozilla Network Security Services (NSS), as used in Google Chrome before 17 on Windows and Mac OS X, might allow local users to gain privileges via a Trojan horse pkcs11.txt file in a top-level directory. NOTE: the vendor's response was "Strange behavior, but we're not treating this as a security bug." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3892 | None | None | Double free vulnerability in the Theora decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3893 | None | None | Google Chrome before 15.0.874.120 does not properly implement the MKV and Vorbis media handlers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3894 | None | None | Google Chrome before 15.0.874.120 does not properly perform VP8 decoding, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted stream.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3895 | None | None | Heap-based buffer overflow in the Vorbis decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3896 | None | None | Buffer overflow in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to shader variable mapping.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3897 | None | None | Use-after-free vulnerability in Google Chrome before 15.0.874.120 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3898 | None | None | Google Chrome before 15.0.874.120, when Java Runtime Environment (JRE) 7 is used, does not request user confirmation before applet execution begins, which allows remote attackers to have an unspecified impact via a crafted applet.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3900 | None | None | Google V8, as used in Google Chrome before 15.0.874.121, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write operation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-4548 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 16.0.912.44 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-5069 | None | None | The Cascading Style Sheets (CSS) implementation in Google Chrome 4 does not properly handle the :visited pseudo-class, which allows remote attackers to obtain sensitive information about visited web pages via a crafted HTML document. NOTE: this may overlap CVE-2010-2264.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2010-5073 | None | None | The JavaScript implementation in Google Chrome 4 does not properly restrict the set of values contained in the object returned by the getComputedStyle method, which allows remote attackers to obtain sensitive information about visited web pages by calling this method. NOTE: this may overlap CVE-2010-5070. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-4691 | None | None | Google Chrome 15.0.874.121 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-4692 | None | None | WebKit, as used in Apple Safari 5.1.1 and earlier and Google Chrome 15 and earlier, does not prevent capture of data about the time required for image loading, which makes it easier for remote attackers to determine whether an image exists in the browser cache via crafted JavaScript code, as demonstrated by visipisi. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-4719 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 16.0.912.63 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3903 | None | None | Google Chrome before 16.0.912.63 does not properly perform regex matching, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3904 | None | None | Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to bidirectional text (aka bidi) handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3905 | None | None | libxml2, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3906 | None | None | The PDF parser in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3907 | None | None | The view-source feature in Google Chrome before 16.0.912.63 allows remote attackers to spoof the URL bar via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3908 | None | None | Google Chrome before 16.0.912.63 does not properly parse SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3909 | None | None | The Cascading Style Sheets (CSS) implementation in Google Chrome before 16.0.912.63 on 64-bit platforms does not properly manage property arrays, which allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3910 | None | None | Google Chrome before 16.0.912.63 does not properly handle YUV video frames, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3911 | None | None | Google Chrome before 16.0.912.63 does not properly handle PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3912 | None | None | Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3913 | None | None | Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to Range handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3914 | None | None | The internationalization (aka i18n) functionality in Google V8, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3915 | None | None | Buffer overflow in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF fonts.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3916 | None | None | Google Chrome before 16.0.912.63 does not properly handle PDF cross references, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3917 | None | None | Stack-based buffer overflow in FileWatcher in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3919 | None | None | Heap-based buffer overflow in libxml2, as used in Google Chrome before 16.0.912.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3921 | None | None | Use-after-free vulnerability in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving animation frames.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3922 | None | None | Stack-based buffer overflow in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to glyph handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-0695 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 17.0.963.27 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3924 | None | None | Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM selections.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3925 | None | None | Use-after-free vulnerability in the Safe Browsing feature in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors related to a navigation entry and an interstitial page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3926 | None | None | Heap-based buffer overflow in the tree builder in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3927 | None | None | Skia, as used in Google Chrome before 16.0.912.77, does not perform all required initialization of values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3928 | None | None | Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3953 | None | None | Google Chrome before 17.0.963.46 does not prevent monitoring of the clipboard after a paste event, which has unspecified impact and remote attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3954 | None | None | Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via vectors that trigger a large amount of database usage.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3955 | None | None | Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that trigger the aborting of an IndexedDB transaction.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3956 | None | None | The extension implementation in Google Chrome before 17.0.963.46 does not properly handle sandboxed origins, which might allow remote attackers to bypass the Same Origin Policy via a crafted extension.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3957 | None | None | Use-after-free vulnerability in the garbage-collection functionality in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF documents. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3958 | None | None | Google Chrome before 17.0.963.46 does not properly perform casts of variables during handling of a column span, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3959 | None | None | Buffer overflow in the locale implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3960 | None | None | Google Chrome before 17.0.963.46 does not properly decode audio data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3961 | None | None | Race condition in Google Chrome before 17.0.963.46 allows remote attackers to execute arbitrary code via vectors that trigger a crash of a utility process.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3962 | None | None | Google Chrome before 17.0.963.46 does not properly perform path clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3963 | None | None | Google Chrome before 17.0.963.46 does not properly handle PDF FAX images, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3964 | None | None | Google Chrome before 17.0.963.46 does not properly implement the drag-and-drop feature, which makes it easier for remote attackers to spoof the URL bar via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3965 | None | None | Google Chrome before 17.0.963.46 does not properly check signatures, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3966 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to error handling for Cascading Style Sheets (CSS) token-sequence data. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3967 | None | None | Unspecified vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via a crafted certificate.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3968 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving Cascading Style Sheets (CSS) token sequences.                         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3969 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout of SVG documents.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3970 | None | None | libxslt, as used in Google Chrome before 17.0.963.46, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3971 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to mousemove events.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3972 | None | None | The shader translator implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3015 | None | None | Multiple integer overflows in the PDF codecs in Google Chrome before 17.0.963.56 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3016 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes, related to a "read-after-free" issue.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3017 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to database handling.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3018 | None | None | Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to path rendering.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3019 | None | None | Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska video (aka MKV) file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3020 | None | None | Unspecified vulnerability in the Native Client validator implementation in Google Chrome before 17.0.963.56 has unknown impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3021 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to subframe loading.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3022 | None | None | translate/translate_manager.cc in Google Chrome before 17.0.963.56 and 19.x before 19.0.1036.7 uses an HTTP session to exchange data for translation, which allows remote attackers to obtain sensitive information by sniffing the network.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3023 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to drag-and-drop operations.                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3024 | None | None | Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service (application crash) via an empty X.509 certificate.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3025 | None | None | Google Chrome before 17.0.963.56 does not properly parse H.264 data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3026 | None | None | Integer overflow in libpng, as used in Google Chrome before 17.0.963.56, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an integer truncation.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3027 | None | None | Google Chrome before 17.0.963.56 does not properly perform a cast of an unspecified variable during handling of columns, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-1418 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 17.0.963.60 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3031 | None | None | Use-after-free vulnerability in the element wrapper in Google V8, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3032 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG values.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3033 | None | None | Buffer overflow in Skia, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3034 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3035 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3036 | None | None | Google Chrome before 17.0.963.65 does not properly perform a cast of an unspecified variable during handling of line boxes, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3037 | None | None | Google Chrome before 17.0.963.65 does not properly perform casts of unspecified variables during the splitting of anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3038 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to multi-column handling.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3039 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to quote handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3040 | None | None | Google Chrome before 17.0.963.65 does not properly handle text, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3041 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of class attributes.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3042 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of table sections.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3043 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a flexbox (aka flexible box) in conjunction with the floating of elements.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3044 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animation elements.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3046 | None | None | The extension subsystem in Google Chrome before 17.0.963.78 does not properly handle history navigation, which allows remote attackers to execute arbitrary code by leveraging a "Universal XSS (UXSS)" issue.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3047 | None | None | The GPU process in Google Chrome before 17.0.963.79 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an error in the plug-in loading mechanism.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3045 | None | None | Integer signedness error in the png_inflate function in pngutil.c in libpng before 1.4.10beta01, as used in Google Chrome before 17.0.963.83 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file, a different vulnerability than CVE-2011-3026. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3050 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the : first-letter pseudo-element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3051 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the cross-fade function.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3052 | None | None | The WebGL implementation in Google Chrome before 17.0.963.83 does not properly handle CANVAS elements, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.                         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3053 | None | None | Use-after-free vulnerability in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to block splitting.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3054 | None | None | The WebUI privilege implementation in Google Chrome before 17.0.963.83 does not properly perform isolation, which allows remote attackers to bypass intended access restrictions via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3055 | None | None | The browser native UI in Google Chrome before 17.0.963.83 does not require user confirmation before an unpacked extension installation, which allows user-assisted remote attackers to have an unspecified impact via a crafted extension.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3056 | None | None | Google Chrome before 17.0.963.83 allows remote attackers to bypass the Same Origin Policy via vectors involving a "magic iframe."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3057 | None | None | Google V8, as used in Google Chrome before 17.0.963.83, allows remote attackers to cause a denial of service via vectors that trigger an invalid read operation.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-1845 | None | None | Use-after-free vulnerability in Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the DEP and ASLR protection mechanisms, and execute arbitrary code, via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-1846 | None | None | Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the sandbox protection mechanism by leveraging access to a sandboxed process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3049 | None | None | Google Chrome before 17.0.963.83 does not properly restrict the extension web request API, which allows remote attackers to cause a denial of service (disrupted system requests) via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3058 | None | None | Google Chrome before 18.0.1025.142 does not properly handle the EUC-JP encoding system, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3059 | None | None | Google Chrome before 18.0.1025.142 does not properly handle SVG text elements, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3060 | None | None | Google Chrome before 18.0.1025.142 does not properly handle text fragments, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3061 | None | None | Google Chrome before 18.0.1025.142 does not properly check X.509 certificates before use of a SPDY proxy, which might allow man-in-the-middle attackers to spoof servers or obtain sensitive information via a crafted certificate.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3062 | None | None | Off-by-one error in the OpenType Sanitizer in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted OpenType file.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3063 | None | None | Google Chrome before 18.0.1025.142 does not properly validate the renderer's navigation requests, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3064 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG clipping.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3065 | None | None | Skia, as used in Google Chrome before 18.0.1025.142, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3066 | None | None | Skia, as used in Google Chrome before 18.0.1025.151, does not properly perform clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3067 | None | None | Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to replacement of IFRAME elements.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3068 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to run-in boxes. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3069 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to line boxes.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3070 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3071 | None | None | Use-after-free vulnerability in the HTMLMediaElement implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3072 | None | None | Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to pop-up windows.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3073 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG resources.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3074 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3075 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style-application commands.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3076 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to focus handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3077 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the script bindings, related to a "read-after-free" issue.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-0724 | None | None | Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0725.       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-0725 | None | None | Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0724.       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-1240 | None | None | Cross-site scripting (XSS) vulnerability in the RECRUIT Dokodemo Rikunabi 2013 extension before 1.0.1 for Google Chrome allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3078 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3081. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3079 | None | None | The Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168, as used in Mozilla Firefox before 38.0 and other products, does not properly validate messages, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3080 | None | None | Race condition in the Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168 allows attackers to bypass intended sandbox restrictions via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3081 | None | None | Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3078.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-1521 | None | None | Use-after-free vulnerability in the XML parser in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3083 | None | None | browser/profiles/profile_impl_io_data.cc in Google Chrome before 19.0.1084.46 does not properly handle a malformed ftp URL in the SRC attribute of a VIDEO element, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted web page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3084 | None | None | Google Chrome before 19.0.1084.46 does not use a dedicated process for the loading of links found on an internal page, which might allow attackers to bypass intended sandbox restrictions via a crafted page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3085 | None | None | The Autofill feature in Google Chrome before 19.0.1084.46 does not properly restrict field values, which allows remote attackers to cause a denial of service (UI corruption) and possibly conduct spoofing attacks via vectors involving long values.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3086 | None | None | Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a STYLE element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3087 | None | None | Google Chrome before 19.0.1084.46 does not properly perform window navigation, which has unspecified impact and remote attack vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3088 | None | None | Google Chrome before 19.0.1084.46 does not properly draw hairlines, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3089 | None | None | Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving tables.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3090 | None | None | Race condition in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker processes.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3091 | None | None | Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3092 | None | None | The regex implementation in Google V8, as used in Google Chrome before 19.0.1084.46, allows remote attackers to cause a denial of service (invalid write operation) or possibly have unspecified other impact via unknown vectors.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3093 | None | None | Google Chrome before 19.0.1084.46 does not properly handle glyphs, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3094 | None | None | Google Chrome before 19.0.1084.46 does not properly handle Tibetan text, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3095 | None | None | The OGG container in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3096 | None | None | Use-after-free vulnerability in Google Chrome before 19.0.1084.46 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an error in the GTK implementation of the omnibox.       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3097 | None | None | The PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an out-of-bounds write error in the implementation of sampled functions. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3098 | None | None | Google Chrome before 19.0.1084.46 on Windows uses an incorrect search path for the Windows Media Player plug-in, which might allow local users to gain privileges via a Trojan horse plug-in in an unspecified directory.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3099 | None | None | Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a malformed name for the font encoding.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3100 | None | None | Google Chrome before 19.0.1084.46 does not properly draw dash paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3101 | None | None | Google Chrome before 19.0.1084.46 on Linux does not properly mitigate an unspecified flaw in an NVIDIA driver, which has unknown impact and attack vectors. NOTE: see CVE-2012-3105 for the related MFSA 2012-34 issue in Mozilla products.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3102 | None | None | Off-by-one error in libxml2, as used in Google Chrome before 19.0.1084.46 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.                                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3103 | None | None | Google V8, as used in Google Chrome before 19.0.1084.52, does not properly perform garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3104 | None | None | Skia, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3105 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the : first-letter pseudo-element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3106 | None | None | The WebSockets implementation in Google Chrome before 19.0.1084.52 does not properly handle use of SSL, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.                                     |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3107 | None | None | Google Chrome before 19.0.1084.52 does not properly implement JavaScript bindings for plug-ins, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3108 | None | None | Use-after-free vulnerability in Google Chrome before 19.0.1084.52 allows remote attackers to execute arbitrary code via vectors related to the browser cache.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3109 | None | None | Google Chrome before 19.0.1084.52 on Linux does not properly perform a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact by leveraging an error in the GTK implementation of the UI.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3110 | None | None | The PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3111 | None | None | Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (invalid read operation) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3112 | None | None | Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an invalid encrypted document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3113 | None | None | The PDF functionality in Google Chrome before 19.0.1084.52 does not properly perform a cast of an unspecified variable during handling of color spaces, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3114 | None | None | Multiple buffer overflows in the PDF functionality in Google Chrome before 19.0.1084.52 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unknown function calls.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-3115 | None | None | Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger "type corruption."  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-3290 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 20.0.1132.22 on the Acer AC700; Samsung Series 5, 5 550, and Chromebox 3; and Cr-48 Chromebook platforms have unknown impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2764 | None | None | Untrusted search path vulnerability in Google Chrome before 20.0.1132.43 on Windows might allow local users to gain privileges via a Trojan horse Metro DLL in the current working directory.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2807 | None | None | Multiple integer overflows in libxml2, as used in Google Chrome before 20.0.1132.43 and other products, on 64-bit Linux platforms allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2815 | None | None | Google Chrome before 20.0.1132.43 allows remote attackers to obtain potentially sensitive information from a fragment identifier by leveraging access to an IFRAME element associated with a different domain.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2816 | None | None | Google Chrome before 20.0.1132.43 on Windows does not properly isolate sandboxed processes, which might allow remote attackers to cause a denial of service (process interference) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2817 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to tables that have sections.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2818 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the layout of documents that use the Cascading Style Sheets (CSS) counters feature.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2819 | None | None | The texSubImage2D implementation in the WebGL subsystem in Google Chrome before 20.0.1132.43 does not properly handle uploads to floating-point textures, which allows remote attackers to cause a denial of service (assertion failure and application crash) or possibly have unspecified other impact via a crafted web page, as demonstrated by certain WebGL performance tests, aka rdar problem 11520387. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2820 | None | None | Google Chrome before 20.0.1132.43 does not properly implement SVG filters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2821 | None | None | The autofill implementation in Google Chrome before 20.0.1132.43 does not properly display text, which has unspecified impact and remote attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2822 | None | None | The PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2823 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG resources.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2824 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG painting.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2825 | None | None | The XSL implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2826 | None | None | Google Chrome before 20.0.1132.43 does not properly implement texture conversion, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2827 | None | None | Use-after-free vulnerability in the UI in Google Chrome before 20.0.1132.43 on Mac OS X allows attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2828 | None | None | Multiple integer overflows in the PDF functionality in Google Chrome before 20.0.1132.43 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2829 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the : first-letter pseudo-element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2830 | None | None | Google Chrome before 20.0.1132.43 does not properly set array values, which allows remote attackers to cause a denial of service (incorrect pointer use) or possibly have unspecified other impact via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2831 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG references.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2832 | None | None | The image-codec implementation in the PDF functionality in Google Chrome before 20.0.1132.43 does not initialize an unspecified pointer, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2833 | None | None | Buffer overflow in the JS API in the PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2834 | None | None | Integer overflow in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted data in the Matroska container format.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2842 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counter handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2843 | None | None | Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout height tracking.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2844 | None | None | The PDF functionality in Google Chrome before 20.0.1132.57 does not properly handle JavaScript code, which allows remote attackers to cause a denial of service (incorrect object access) or possibly have unspecified other impact via a crafted document.       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4050 | None | None | Multiple unspecified vulnerabilities in Google Chrome OS before 21.0.1180.50 on the Cr-48 and Samsung Series 5 and 5 550 Chromebook platforms, and the Samsung Chromebox Series 3, have unknown impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2846 | None | None | Google Chrome before 21.0.1180.57 on Linux does not properly isolate renderer processes, which allows remote attackers to cause a denial of service (cross-process interference) via unspecified vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2847 | None | None | Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not request user confirmation before continuing a large series of downloads, which allows user-assisted remote attackers to cause a denial of service (resource consumption) via a crafted web site.       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2848 | None | None | The drag-and-drop implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to bypass intended file access restrictions via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2849 | None | None | Off-by-one error in the GIF decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2850 | None | None | Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to have an unknown impact via a crafted document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2851 | None | None | Multiple integer overflows in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2852 | None | None | The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly handle object linkage, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2853 | None | None | The webRequest API in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly interact with the Chrome Web Store, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.        |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2854 | None | None | Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to obtain potentially sensitive information about pointer values by leveraging access to a WebUI renderer process.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2855 | None | None | Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2856 | None | None | The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2857 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) DOM implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2858 | None | None | Buffer overflow in the WebP decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted WebP image.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2859 | None | None | Google Chrome before 21.0.1180.57 on Linux does not properly handle tabs, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2860 | None | None | The date-picker implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2862 | None | None | Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2863 | None | None | The PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2864 | None | None | Mesa, as used in Google Chrome before 21.0.1183.0 on the Acer AC700, Cr-48, and Samsung Series 5 and 5 550 Chromebook platforms, and the Samsung Chromebox Series 3, allows remote attackers to execute arbitrary code via unspecified vectors that trigger an "array overflow."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1398 | None | None | The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2865 | None | None | Google Chrome before 21.0.1180.89 does not properly perform line breaking, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2866 | None | None | Google Chrome before 21.0.1180.89 does not properly perform a cast of an unspecified variable during handling of run-in elements, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2867 | None | None | The SPDY implementation in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2868 | None | None | Race condition in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving improper interaction between worker processes and an XMLHttpRequest (aka XHR) object.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2869 | None | None | Google Chrome before 21.0.1180.89 does not properly load URLs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a "stale buffer."  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2870 | None | None | libxslt 1.1.26 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly manage memory, which might allow remote attackers to cause a denial of service (application crash) via a crafted XSLT expression that is not properly identified during XPath navigation, related to (1) the xsltCompileLocationPathPattern function in libxslt/pattern.c and (2) the xsltGenerateIdFunction function in libxslt/functions.c.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2871 | None | None | libxml2 2.9.0-rc1 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly support a cast of an unspecified variable during handling of XSL transforms, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document, related to the _xmlNs data structure in include/libxml/tree.h.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2872 | None | None | Cross-site scripting (XSS) vulnerability in an SSL interstitial page in Google Chrome before 21.0.1180.89 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4388 | None | None | The sapi_header_op function in main/SAPI.c in PHP 5.4.0RC2 through 5.4.0 does not properly determine a pointer during checks for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-1398. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4903 | None | None | Google Chrome before 18.0.1025308 on Android does not properly restrict access to file: URLs, which allows remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by obtaining credential data, a different vulnerability than CVE-2012-4906.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4904 | None | None | Cross-application scripting vulnerability in Google Chrome before 18.0.1025308 on Android allows remote attackers to inject arbitrary web script via unspecified vectors, as demonstrated by "Universal XSS (UXSS)" attacks against the current tab.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4905 | None | None | Cross-site scripting (XSS) vulnerability in Google Chrome before 18.0.1025308 on Android allows remote attackers to inject arbitrary web script or HTML via an extra in an Intent object, aka "Universal XSS (UXSS)."  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4906 | None | None | Google Chrome before 18.0.1025308 on Android does not properly restrict access to file: URLs, which allows remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by obtaining credential data, a different vulnerability than CVE-2012-4903.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4907 | None | None | Google Chrome before 18.0.1025308 on Android does not properly restrict access from JavaScript code to Android APIs, which allows remote attackers to have an unspecified impact via a crafted web page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4908 | None | None | Google Chrome before 18.0.1025308 on Android allows remote attackers to bypass the Same Origin Policy and obtain access to local files via vectors involving a symlink.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4909 | None | None | Google Chrome before 18.0.1025308 on Android allows remote attackers to obtain cookie information via a crafted application.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4929 | None | None | The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-4930 | None | None | The SPDY protocol 3 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, can perform TLS encryption of compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2874 | None | None | Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2883.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2875 | None | None | Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 22.0.1229.79 allow remote attackers to have an unknown impact via a crafted document.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2876 | None | None | Buffer overflow in the SSE2 optimization functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2877 | None | None | The extension system in Google Chrome before 22.0.1229.79 does not properly handle modal dialogs, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2878 | None | None | Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2879 | None | None | Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service (DOM topology corruption) via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2880 | None | None | Race condition in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the plug-in paint buffer.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2881 | None | None | Google Chrome before 22.0.1229.79 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2882 | None | None | FFmpeg, as used in Google Chrome before 22.0.1229.79, does not properly handle OGG containers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "wild pointer" issue. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2883 | None | None | Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2874. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2884 | None | None | Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2885 | None | None | Double free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to application exit.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2886 | None | None | Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors related to the Google V8 bindings, aka "Universal XSS (UXSS)."                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2887 | None | None | Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving onclick events.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2888 | None | None | Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG text references.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2889 | None | None | Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors involving frames, aka "Universal XSS (UXSS)."                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2890 | None | None | Use-after-free vulnerability in the PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2891 | None | None | The IPC implementation in Google Chrome before 22.0.1229.79 allows attackers to obtain potentially sensitive information about memory addresses via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2892 | None | None | Unspecified vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to bypass the pop-up blocker via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2893 | None | None | Double free vulnerability in libxslt, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XSL transforms.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2894 | None | None | Google Chrome before 22.0.1229.79 does not properly handle graphics-context data structures, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2895 | None | None | The PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.                         |

|               |                    |               |          |      |   |
|---------------|--------------------|---------------|----------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2896 | None     | None | Integer overflow in the WebGL implementation in Google Chrome before 22.0.1229.79 on Mac OS X allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2897 | HIGH     | 7.8  | The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT, as used by Google Chrome before 22.0.1229.79 and other programs, do not properly handle objects in memory, which allows remote attackers to execute arbitrary code via a crafted TrueType font file, aka "Windows Font Parsing Vulnerability" or "TrueType Font Parsing Vulnerability." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2900 | None     | None | Skia, as used in Google Chrome before 22.0.1229.92, does not properly render text, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5108 | None     | None | Race condition in Google Chrome before 22.0.1229.92 allows remote attackers to execute arbitrary code via vectors related to audio devices.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5109 | None     | None | The International Components for Unicode (ICU) functionality in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a regular expression.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5110 | None     | None | The compositor in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5111 | None     | None | Google Chrome before 22.0.1229.92 does not monitor for crashes of Pepper plug-ins, which has unspecified impact and remote attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5112 | None     | None | Use-after-free vulnerability in the SVG implementation in WebKit, as used in Google Chrome before 22.0.1229.94, allows remote attackers to execute arbitrary code via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5376 | CRITICAL | 9.6  | The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended sandbox restrictions and write to arbitrary files by leveraging access to a renderer process, a different vulnerability than CVE-2012-5112.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5115 | None | None | Google Chrome before 23.0.1271.64 on Mac OS X does not properly mitigate improper write behavior in graphics drivers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger "wild writes."       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5116 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG filters.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5117 | None | None | Google Chrome before 23.0.1271.64 does not properly restrict the loading of an SVG subresource in the context of an IMG element, which has unspecified impact and remote attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5118 | None | None | Google Chrome before 23.0.1271.64 on Mac OS X does not properly validate an integer value during the handling of GPU command buffers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5119 | None | None | Race condition in Pepper, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to buffers.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5120 | None | None | Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, on 64-bit Linux platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to an array. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5121 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video layout.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5122 | None | None | Google Chrome before 23.0.1271.64 does not properly perform a cast of an unspecified variable during handling of input, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5123 | None | None | Skia, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5124 | None | None | Google Chrome before 23.0.1271.64 does not properly handle textures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5125 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5126 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of plug-in placeholders.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5127 | None | None | Integer overflow in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted WebP image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5128 | None | None | Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, does not properly perform write operations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5851 | None | None | html/parser/XSSAuditor.cpp in WebCore in WebKit, as used in Google Chrome through 22 and Safari 5.1.7, does not consider all possible output contexts of reflected data, which makes it easier for remote attackers to bypass a cross-site scripting (XSS) protection mechanism via a crafted string, aka rdar problem 12019108. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5130 | None | None | Skia, as used in Google Chrome before 23.0.1271.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5131 | None | None | Google Chrome before 23.0.1271.91 on Mac OS X does not properly mitigate improper rendering behavior in the Intel GPU driver, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5132 | None | None | Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service (application crash) via a response with chunked transfer coding.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5133 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5134 | None | None | Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome before 23.0.1271.91 and other products, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5135 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5136 | None | None | Google Chrome before 23.0.1271.91 does not properly perform a cast of an unspecified variable during handling of the INPUT element, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5129 | None | None | Heap-based buffer overflow in the WebGL subsystem in Google Chrome OS before 23.0.1271.94 allows remote attackers to cause a denial of service (GPU process crash) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5137 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Media Source API.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5138 | None | None | Google Chrome before 23.0.1271.95 does not properly handle file paths, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5139 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to visibility events.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5140 | None | None | Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the URL loader.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5141 | None | None | Google Chrome before 23.0.1271.97 does not properly restrict instantiation of the Chromoting client plug-in, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5142 | None | None | Google Chrome before 23.0.1271.97 does not properly handle history navigation, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5143 | None | None | Integer overflow in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PPAPI image buffers.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5144 | None | None | Google Chrome before 23.0.1271.97, and Libav 0.7.x before 0.7.7 and 0.8.x before 0.8.5, do not properly perform AAC decoding, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via vectors related to "an off-by-one overwrite when switching to LTP profile from MAIN." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5145 | None | None | Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG layout.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5146 | None | None | Google Chrome before 24.0.1312.52 allows remote attackers to bypass the Same Origin Policy via a malformed URL.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5147 | None | None | Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5148 | None | None | The hyphenation functionality in Google Chrome before 24.0.1312.52 does not properly validate file names, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5149 | None | None | Integer overflow in the audio IPC layer in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5150 | None | None | Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving seek operations on video data.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5151 | None | None | Integer overflow in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code in a PDF document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5152 | None | None | Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving seek operations on video data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5153 | None | None | Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to stack memory.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5154 | None | None | Integer overflow in Google Chrome before 24.0.1312.52 on Windows allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to allocation of shared memory.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5155 | None | None | Google Chrome before 24.0.1312.52 on Mac OS X does not use an appropriate sandboxing approach for worker processes, which makes it easier for remote attackers to bypass intended access restrictions via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5156 | None | None | Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF fields.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-5157 | None | None | Google Chrome before 24.0.1312.52 does not properly handle image data in PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0828 | None | None | The PDF functionality in Google Chrome before 24.0.1312.52 does not properly perform a cast of an unspecified variable during processing of the root of the structure tree, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0829 | None | None | Google Chrome before 24.0.1312.52 does not properly maintain database metadata, which allows remote attackers to bypass intended file-access restrictions via unspecified vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0830 | None | None | The IPC layer in Google Chrome before 24.0.1312.52 on Windows omits a NUL character required for termination of an unspecified data structure, which has unknown impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0831 | None | None | Directory traversal vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to have an unspecified impact by leveraging access to an extension process.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0832 | None | None | Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0833 | None | None | Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to printing.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0834 | None | None | Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving glyphs.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0835 | None | None | Unspecified vulnerability in the Geolocation implementation in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (application crash) via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0836 | None | None | Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, does not properly implement garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0837 | None | None | Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0838 | None | None | Google Chrome before 24.0.1312.52 on Linux uses weak permissions for shared memory segments, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0839 | None | None | Use-after-free vulnerability in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of fonts in CANVAS elements.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0840 | None | None | Google Chrome before 24.0.1312.56 does not validate URLs during the opening of new windows, which has unspecified impact and remote attack vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0841 | None | None | Array index error in the content-blocking functionality in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0842 | None | None | Google Chrome before 24.0.1312.56 does not properly handle %00 characters in pathnames, which has unspecified impact and attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0843 | None | None | content/renderer/media/webrtc_audio_renderer.cc in Google Chrome before 24.0.1312.56 on Mac OS X does not use an appropriate buffer size for the 96 kHz sampling rate, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a web site that provides WebRTC audio.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-1489 | None | None | Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 10 and Update 11, when running on Windows using Internet Explorer, Firefox, Opera, and Google Chrome, allows remote attackers to bypass the "Very High" security level of the Java Control Panel and execute unsigned Java code without prompting the user via unknown vectors, aka "Issue 53" and the "Java Security Slider" vulnerability. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0879 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly implement web audio nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0880 | None | None | Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to databases.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0881 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via crafted data in the Matroska container format.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0882 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via a large number of SVG parameters.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0883 | None | None | Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0884 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly load Native Client (aka NaCl) code, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0885 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict API privileges during interaction with the Chrome Web Store, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0886 | None | None | Google Chrome before 25.0.1364.99 on Mac OS X does not properly implement signal handling for Native Client (aka NaCl) code, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0887 | None | None | The developer-tools process in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict privileges during interaction with a connected server, which has unspecified impact and attack vectors.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0888 | None | None | Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a "user gesture check for dangerous file downloads."                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0889 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly enforce a user gesture requirement before proceeding with a file download, which might make it easier for remote attackers to execute arbitrary code via a crafted file. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0890 | None | None | Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service (memory corruption) or possibly have other impact via unknown vectors.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0891 | None | None | Integer overflow in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a blob.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0892 | None | None | Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0893 | None | None | Race condition in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0894 | None | None | Buffer overflow in the vorbis_parse_setup_hdr_floors function in the Vorbis decoder in vorbisdec.c in libavcodec in FFmpeg through 1.1.3, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (divide-by-zero error or out-of-bounds array access) or possibly have unspecified other impact via vectors involving a zero value for a bark map size. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0895 | None | None | Google Chrome before 25.0.1364.97 on Linux, and before 25.0.1364.99 on Mac OS X, does not properly handle pathnames during copy operations, which might make it easier for remote attackers to execute arbitrary programs via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0896 | None | None | Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly manage memory during message handling for plug-ins, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0897 | None | None | Off-by-one error in the PDF functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0898 | None | None | Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a URL.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0899 | None | None | Integer overflow in the padding implementation in the opus_packet_parse_impl function in src/opus_decoder.c in Opus before 1.0.2, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a long packet. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0900 | None | None | Race condition in the International Components for Unicode (ICU) functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2268 | None | None | Unspecified vulnerability in the MathML implementation in WebKit in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, has unknown impact and remote attack vectors, related to a "high severity security issue."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0902 | None | None | Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0903 | None | None | Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of browser navigation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0904 | None | None | The Web Audio implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0905 | None | None | Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG animation.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0906 | None | None | The IndexedDB implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0907 | None | None | Race condition in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media threads.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0908 | None | None | Google Chrome before 25.0.1364.152 does not properly manage bindings of extension processes, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0909 | None | None | The XSS Auditor in Google Chrome before 25.0.1364.152 allows remote attackers to obtain sensitive HTTP Referer information via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0910 | None | None | Google Chrome before 25.0.1364.152 does not properly manage the interaction between the browser process and renderer processes during authorization of the loading of a plug-in, which makes it easier for remote attackers to bypass intended access restrictions via vectors involving a blocked plug-in.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0911 | None | None | Directory traversal vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to have an unspecified impact via vectors related to databases.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2493 | None | None | The Hook_Terminate function in chrome_frame/protocol_sink_wrap.cc in the Google Chrome Frame plugin before 26.0.1410.28 for Internet Explorer does not properly handle attach tab requests, which allows user-assisted remote attackers to cause a denial of service (application crash) via an _blank value for the target attribute of an A element.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0912 | None | None | WebKit in Google Chrome before 25.0.1364.160 allows remote attackers to execute arbitrary code via vectors that leverage "type confusion."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0913 | None | None | Integer overflow in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the i915 driver in the Direct Rendering Manager (DRM) subsystem in the Linux kernel through 3.8.3, as used in Google Chrome OS before 25.0.1364.173 and other products, allows local users to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted application that triggers many relocation copies, and potentially leads to a race condition. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0915 | None | None | The GPU process in Google Chrome OS before 25.0.1364.173 allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to an "overflow."  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2632 | None | None | Google V8 before 3.17.13, as used in Google Chrome before 27.0.1444.3, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by the Bejeweled game. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0916 | None | None | Use-after-free vulnerability in the Web Audio implementation in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0917 | None | None | The URL loader in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0918 | None | None | Google Chrome before 26.0.1410.43 does not prevent navigation to developer tools in response to a drag-and-drop operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0919 | None | None | Use-after-free vulnerability in Google Chrome before 26.0.1410.43 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the presence of an extension that creates a pop-up window.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0920 | None | None | Use-after-free vulnerability in the extension bookmarks API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0921 | None | None | The Isolated Sites feature in Google Chrome before 26.0.1410.43 does not properly enforce the use of separate processes, which makes it easier for remote attackers to bypass intended access restrictions via a crafted web site.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0922 | None | None | Google Chrome before 26.0.1410.43 does not properly restrict brute-force access attempts against web sites that require HTTP Basic Authentication, which has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0923 | None | None | The USB Apps API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0924 | None | None | The extension functionality in Google Chrome before 26.0.1410.43 does not verify that use of the permissions API is consistent with file permissions, which has unspecified impact and attack vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0925 | None | None | Google Chrome before 26.0.1410.43 does not ensure that an extension has the tabs (aka <code>APIPermission::kTab</code> ) permission before providing a URL to this extension, which has unspecified impact and remote attack vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0926 | None | None | Google Chrome before 26.0.1410.43 does not properly handle active content in an <code>EMBED</code> element during a copy-and-paste operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-0927 | None | None | Google Chrome OS before 26.0.1410.57 relies on a Pango <code>pango-utils.c read_config</code> implementation that loads the contents of the <code>.pangorc</code> file in the user's home directory, and the file referenced by the <code>PANGO_RC_FILE</code> environment variable, which allows attackers to bypass intended access restrictions via crafted configuration data. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2832 | None | None | The <code>Buffer::Set</code> function in <code>core/cross/buffer.cc</code> in the O3D plug-in in Google Chrome OS before 26.0.1410.57 does not prevent uninitialized data from remaining in a buffer, which might allow remote attackers to obtain sensitive information via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2833 | None | None | Use-after-free vulnerability in the O3D plug-in in Google Chrome OS before 26.0.1410.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper management of ownership relationships involving <code>Elements</code> and <code>DrawElements</code> .   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2834 | None | None | Google Chrome OS before 26.0.1410.57 does not properly enforce origin restrictions for the O3D and Google Talk plug-ins, which allows remote attackers to bypass the domain-whitelist protection mechanism via a crafted web site, a different vulnerability than CVE-2013-2835.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2835 | None | None | Google Chrome OS before 26.0.1410.57 does not properly enforce origin restrictions for the O3D and Google Talk plug-ins, which allows remote attackers to bypass the domain-whitelist protection mechanism via a crafted web site, a different vulnerability than CVE-2013-2834.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2836 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.93 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2837 | None | None | Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2838 | None | None | Google V8, as used in Google Chrome before 27.0.1453.93, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2839 | None | None | Google Chrome before 27.0.1453.93 does not properly perform a cast of an unspecified variable during handling of clipboard data, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2840 | None | None | Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2846.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2841 | None | None | Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of Pepper resources.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2842 | None | None | Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of widgets.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2843 | None | None | Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of speech data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2844 | None | None | Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style resolution. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2845 | None | None | The Web Audio implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2846 | None | None | Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2840. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2847 | None | None | Race condition in the workers implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via unknown vectors.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2848 | None | None | The XSS Auditor in Google Chrome before 27.0.1453.93 might allow remote attackers to obtain sensitive information via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2849 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome before 27.0.1453.93 allow user-assisted remote attackers to inject arbitrary web script or HTML via vectors involving a (1) drag-and-drop or (2) copy-and-paste operation.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2854 | None | None | Google Chrome before 27.0.1453.110 on Windows provides an incorrect handle to a renderer process in unspecified circumstances, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2855 | None | None | The Developer Tools API in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2856 | None | None | Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2857 | None | None | Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of images.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2858 | None | None | Use-after-free vulnerability in the HTML5 Audio implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2859 | None | None | Google Chrome before 27.0.1453.110 allows remote attackers to bypass the Same Origin Policy and trigger namespace pollution via unspecified vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2860 | None | None | Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving access to a database API by a worker process.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2861 | None | None | Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2862 | None | None | Skia, as used in Google Chrome before 27.0.1453.110, does not properly handle GPU acceleration, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2863 | None | None | Google Chrome before 27.0.1453.110 does not properly handle SSL sockets, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2864 | None | None | The PDF functionality in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2865 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.110 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2866 | None | None | The Flash plug-in in Google Chrome before 27.0.1453.116, as used on Google Chrome OS before 27.0.1453.116 and separately, does not properly determine whether a user wishes to permit camera or microphone access by a Flash application, which allows remote attackers to obtain sensitive information from a machine's physical environment via a clickjacking attack, as demonstrated by an attack using a crafted Cascading Style Sheets (CSS) opacity property. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2853 | None | None | The HTTPS implementation in Google Chrome before 28.0.1500.71 does not ensure that headers are terminated by <code>\r\n\r\n</code> (carriage return, newline, carriage return, newline), which allows man-in-the-middle attackers to have an unspecified impact via vectors that trigger header truncation.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2867 | None | None | Google Chrome before 28.0.1500.71 does not properly prevent pop-under windows, which allows remote attackers to have an unspecified impact via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2868 | None | None | common/extensions/sync_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2869 | None | None | Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted JPEG2000 image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2870 | None | None | Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote servers to execute arbitrary code via crafted response traffic after a URL request.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2871 | None | None | Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2872 | None | None | Google Chrome before 28.0.1500.71 on Mac OS X does not ensure a sufficient source of entropy for renderer processes, which might make it easier for remote attackers to defeat cryptographic protection mechanisms in third-party components via unspecified vectors.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2873 | None | None | Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a 404 HTTP status code during the loading of resources.                                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2874 | None | None | Google Chrome before 28.0.1500.71 on Windows, when an Nvidia GPU is used, allows remote attackers to bypass intended restrictions on access to screen data via vectors involving IPC transmission of GL textures.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2875 | None | None | core/rendering/svg/SVGInlineTextBox.cpp in the SVG implementation in Blink, as used in Google Chrome before 28.0.1500.71, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2876 | None | None | browser/extensions/api/tabs/tabs_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2877 | None | None | parser.c in libxml2 before 2.9.0, as used in Google Chrome before 28.0.1500.71 and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a document that ends abruptly, related to the lack of certain checks for the XML_PARSER_EOF state.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2878 | None | None | Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the handling of text.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2879 | None | None | Google Chrome before 28.0.1500.71 does not properly determine the circumstances in which a renderer process can be considered a trusted process for sign-in and subsequent sync operations, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site.                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2880 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2881 | None | None | Google Chrome before 28.0.1500.95 does not properly handle frames, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2882 | None | None | Google V8, as used in Google Chrome before 28.0.1500.95, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2883 | None | None | Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to deleting the registration of a MutationObserver object.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2884 | None | None | Use-after-free vulnerability in the DOM implementation in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper tracking of which document owns an Attr object.                                      |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2885 | None | None | Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to not properly considering focus during the processing of JavaScript events in the presence of a multiple-fields input type.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2886 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.95 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2887 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 29.0.1547.57 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2900 | None | None | The FilePath::ReferencesParent function in files/file_path.cc in Google Chrome before 29.0.1547.57 on Windows does not properly handle pathname components composed entirely of . (dot) and whitespace characters, which allows remote attackers to conduct directory traversal attacks via a crafted directory name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2901 | None | None | Multiple integer overflows in (1) libGLESv2/renderer/Renderer9.cpp and (2) libGLESv2/renderer/Renderer11.cpp in Almost Native Graphics Layer Engine (ANGLE), as used in Google Chrome before 29.0.1547.57, allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2902 | None | None | Use-after-free vulnerability in the XSLT ProcessingInstruction implementation in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to an applyXSLTransform call involving (1) an HTML document or (2) an xsl:processing-instructi on element that is still in the process of loading. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2903 | None | None | Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving moving a (1) AUDIO or (2) VIDEO element between documents.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2904 | None | None | Use-after-free vulnerability in the Document::finishedParsing function in core/dom/Document.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via an onload event that changes an IFRAME element so that its src attribute is no longer an XML document, leading to unintended garbage collection of this document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2905 | None | None | The SharedMemory::Create function in memory/shared_memory_posix.cc in Google Chrome before 29.0.1547.57 uses weak permissions under /dev/shm/, which allows attackers to obtain sensitive information via direct access to a POSIX shared-memory file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2906 | None | None | Multiple race conditions in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to threading in core/html/HTMLMediaElement.cpp, core/platform/audio/AudioDSPKernelProcessor.cpp, core/platform/audio/HRTFElevation.cpp, and modules/webaudio/ConvolverNode.cpp.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2907 | None | None | The Window.prototype object implementation in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2908 | None | None | Google Chrome before 30.0.1599.66 uses incorrect function calls to determine the values of NavigationEntry objects, which allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2909 | None | None | Use-after-free vulnerability in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to inline-block rendering for bidirectional Unicode text in an element isolated from its siblings.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2910 | None | None | Use-after-free vulnerability in modules/webaudio/AudioScheduledSourceNode.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2911 | None | None | Use-after-free vulnerability in the XSLStyleSheet::compileStyleSheet function in core/xml/XSLStyleSheetLibxslt.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of post-failure recompilation in unspecified libxslt versions. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2912 | None | None | Use-after-free vulnerability in the PepperInProcessRouter::SendToHost function in content/renderer/pepper/pepper_in_process_router.c in the Pepper Plug-in API (PPAPI) in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a resource-destruction message.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2913 | None | None | Use-after-free vulnerability in the XMLDocumentParser::append function in core/xml/parser/XMLDocumentParser.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an XML document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2914 | None | None | Use-after-free vulnerability in the color-chooser dialog in Google Chrome before 30.0.1599.66 on Windows allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to color_chooser_dialog.cc and color_chooser_win.cc in browser/ui/views/.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2915 | None | None | Google Chrome before 30.0.1599.66 preserves pending NavigationEntry objects in certain invalid circumstances, which allows remote attackers to spoof the address bar via a URL with a malformed scheme, as demonstrated by a nonexistent:12121 URL.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2916 | None | None | Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code, in conjunction with a delay in notifying the user of an attempted spoof.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2917 | None | None | The ReverbConvolverStage::ReverbConvolverStage function in core/platform/audio/ReverbConvolverStage.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the impulseResponse array.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2918 | None | None | Use-after-free vulnerability in the <code>RenderBlock::collapseAnonymousBlockChild</code> function in <code>core/rendering/RenderBlock.cpp</code> in the DOM implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect handling of parent-child relationships for anonymous blocks. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2919 | None | None | Google V8, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2920 | None | None | The <code>DoResolveRelativeHost</code> function in <code>url/url_canon_relative.cc</code> in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via a relative URL containing a hostname, as demonstrated by a protocol-relative URL beginning with a <code>//www.google.com/</code> substring.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2921 | None | None | Double free vulnerability in the <code>ResourceFetcher::didLoadResource</code> function in <code>core/fetch/ResourceFetcher.cpp</code> in the resource loader in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering certain callback processing during the reporting of a resource entry.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2922 | None | None | Use-after-free vulnerability in <code>core/html/HTMLTemplateElement.cpp</code> in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that operates on a <code>TEMPLATE</code> element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2923 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.66 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2924 | None | None | Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before 30.0.1599.66 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2925 | None | None | Use-after-free vulnerability in core/xml/XMLHttpRequest.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger multiple conflicting uses of the same XMLHttpRequest object.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2926 | None | None | Use-after-free vulnerability in the IndentOutdentCommand::tryIndentingAsListItem function in core/editing/IndentOutdentCommand.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to list elements.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2927 | None | None | Use-after-free vulnerability in the HTMLFormElement::prepareForSubmission function in core/html/HTMLFormElement.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to submission for FORM elements.                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2928 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-2931 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.48 allow attackers to execute arbitrary code or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6621 | None | None | Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the x-webkit-speech attribute in a text INPUT element.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6622 | None | None | Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the movement of a media element between documents. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6623 | None | None | The SVG implementation in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging the use of tree order, rather than transitive dependency order, for layout.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6624 | None | None | Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the string values of id attributes.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6625 | None | None | Use-after-free vulnerability in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of DOM range objects in circumstances that require child node removal after a (1) mutation or (2) blur event. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6626 | None | None | The WebContentsImpl::AttachInterstitialPage function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 31.0.1650.48 does not cancel JavaScript dialogs upon generating an interstitial warning, which allows remote attackers to spoof the address bar via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6627 | None | None | net/http/http_stream_parser.cc in Google Chrome before 31.0.1650.48 does not properly process HTTP Informational (aka 1xx) status codes, which allows remote web servers to cause a denial of service (out-of-bounds read) via a crafted response.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6628 | None | None | net/socket/ssl_client_socket_nss.cc in the TLS implementation in Google Chrome before 31.0.1650.48 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which might allow remote web servers to interfere with trust relationships by renegotiating a session.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6632 | None | None | Integer overflow in Google Chrome before 31.0.1650.57 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6802 | None | None | Google Chrome before 31.0.1650.57 allows remote attackers to bypass intended sandbox restrictions by leveraging access to a renderer process, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013, a different vulnerability than CVE-2013-6632.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6629 | None | None | The get_sos function in jdmarker.c in (1) libjpeg 6b and (2) libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48, Ghostscript, and other products, does not check for certain duplications of component data during the reading of segments that follow Start Of Scan (SOS) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.                         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6630 | None | None | The get_dht function in jdmarker.c in libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48 and other products, does not set all elements of a certain Huffman value array during the reading of segments that follow Define Huffman Table (DHT) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6631 | None | None | Use-after-free vulnerability in the Channel::SendRTCPPacket function in voice_engine/channel.cc in libjingle in WebRTC, as used in Google Chrome before 31.0.1650.48 and other products, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger the absence of certain statistics initialization, leading to the skipping of a required DeRegisterExternalTransport call. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6634 | None | None | The OneClickSignInHelper::ShowInfoBarIfPossible function in browser/ui/sync/one_click_signin_helper.cc in Google Chrome before 31.0.1650.63 uses an incorrect URL during realm validation, which allows remote attackers to conduct session fixation attacks and hijack web sessions by triggering improper sync after a 302 (aka Found) HTTP status code.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6635 | None | None | Use-after-free vulnerability in the editing implementation in Blink, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that triggers removal of a node during processing of the DOM tree, related to CompositeEditCommand.cpp and ReplaceSelectionCommand.cpp.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6636 | None | None | The FrameLoader::notifyIfInitialDocumentAccessed function in core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 31.0.1650.63, makes an incorrect check for an empty document during presentation of a modal dialog, which allows remote attackers to spoof the address bar via vectors involving the document.write method.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6637 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.63 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6638 | None | None | Multiple buffer overflows in runtime.cc in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large typed array, related to the (1) Runtime_TypedArrayInitialize and (2) Runtime_TypedArrayInitializeFromArrayLike functions.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6639 | None | None | The DehoistArrayIndex function in hydrogen-dehoist.cc (aka hydrogen.cc) in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via JavaScript code that sets the value of an array element with a crafted index.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6640 | None | None | The DehoistArrayIndex function in hydrogen-dehoist.cc (aka hydrogen.cc) in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service (out-of-bounds read) via JavaScript code that sets a variable to the value of an array element with a crafted index.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2898 | None | None | Google Chrome before 21.0.1180.82 on iOS on iPad devices allows remote attackers to spoof the Omnibox URL via vectors involving SSL error messages, a related issue to CVE-2012-0674.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2012-2899 | None | None | Google Chrome before 21.0.1180.82 on iOS makes certain incorrect calls to WebView methods that trigger use of an applewebdata: URL, which allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks via vectors involving the document.write method.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6641 | None | None | Use-after-free vulnerability in the FormAssociatedElement::formRemovedFromTree function in core/html/FormAssociatedElement.cpp in Blink, as used in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of the past names map of a FORM element. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6642 | None | None | Google Chrome through 32.0.1700.23 on Android allows remote attackers to spoof the address bar via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6643 | None | None | The OneClickSigninBubbleView::WindowClosing function in browser/ui/views/sync/one_click_signin_bubble_view.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6644 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6645 | None | None | Use-after-free vulnerability in the OnWindowRemovingFromRootWindow function in content/browser/web_contents/web_contents_view_aura.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving certain print-preview and tab-switch actions that interact with a speech input element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6646 | None | None | Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the shutting down of a worker process.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6649 | None | None | Use-after-free vulnerability in the RenderSVGImage::paint function in core/rendering/svg/RenderSVGImage.cpp in Blink, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a zero-size SVG image.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6650 | None | None | The StoreBuffer::ExemptPopularPages function in store-buffer.cc in Google V8 before 3.22.24.16, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors that trigger incorrect handling of "popular pages."  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1681 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.102 have unknown impact and attack vectors, related to 12 "security fixes [that were not] either contributed by external researchers or particularly interesting."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6166 | None | None | Google Chrome before 29 sends HTTP Cookie headers without first validating that they have the required character-set restrictions, which allows remote attackers to conduct the equivalent of a persistent Logout CSRF attack via a crafted parameter that forces a web application to set a malformed cookie within an HTTP response.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6652 | None | None | Directory traversal vulnerability in sandbox/win/src/named_pipe_dispatcher.cc in Google Chrome before 33.0.1750.117 on Windows allows attackers to bypass intended named-pipe policy restrictions in the sandbox via vectors related to (1) lack of checks for .. (dot dot) sequences or (2) lack of use of the \\?\ protection mechanism.    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6653 | None | None | Use-after-free vulnerability in the web contents implementation in Google Chrome before 33.0.1750.117 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attempted conflicting access to the color chooser.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6654 | None | None | The SVGAnimateElement::calculateAnimatedValue function in core/svg/SVGAnimateElement.cpp in Blink, as used in Google Chrome before 33.0.1750.117, does not properly handle unexpected data types, which allows remote attackers to cause a denial of service (incorrect cast) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6655 | None | None | Use-after-free vulnerability in Blink, as used in Google Chrome before 33.0.1750.117, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper handling of overflowchanged DOM events during interaction between JavaScript and layout.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6656 | None | None | The XSSAuditor::init function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, processes POST requests by using the body of a redirecting page instead of the body of a redirect target, which allows remote attackers to obtain sensitive information via unspecified vectors. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6657 | None | None | core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, inserts the about:blank URL during certain blocking of FORM elements within HTTP requests, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6658 | None | None | Multiple use-after-free vulnerabilities in the layout implementation in Blink, as used in Google Chrome before 33.0.1750.117, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving (1) running JavaScript code during execution of the updateWidgetPositions function or (2) making a call into a plugin during execution of the updateWidgetPositions function. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6659 | None | None | The SSLClientSocketNSS::Core::OwnAuthCertHandler function in net/socket/ssl_client_socket_nss.cc in Google Chrome before 33.0.1750.117 does not prevent changes to server X.509 certificates during renegotiations, which allows remote SSL servers to trigger use of a new certificate chain, inconsistent with the user's expectations, by initiating a TLS renegotiation.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6660 | None | None | The drag-and-drop implementation in Google Chrome before 33.0.1750.117 does not properly restrict the information in WebDropData data structures, which allows remote attackers to discover full pathnames via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6661 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.117 allow attackers to bypass the sandbox protection mechanism after obtaining renderer access, or have other impact, via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6663 | None | None | Use-after-free vulnerability in the SVGImage::setContainerSize function in core/svg/graphics/SVGImage.cpp in the SVG implementation in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the resizing of a view.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6664 | None | None | Use-after-free vulnerability in the <code>FormAssociatedElement::formRemovedFromTree</code> function in <code>core/html/FormAssociatedElement.cpp</code> in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving FORM elements, as demonstrated by use of the speech-recognition feature.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6665 | None | None | Heap-based buffer overflow in the <code>ResourceProvider::InitializeSoftware</code> function in <code>cc/resources/resource_provider.cc</code> in Google Chrome before 33.0.1750.146 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large texture size that triggers improper memory allocation in the software renderer.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6666 | None | None | The <code>PepperFlashRendererHost::OnNavigate</code> function in <code>renderer/pepper/pepper_flash_renderer_host.cc</code> in Google Chrome before 33.0.1750.146 does not verify that all headers are Cross-Origin Resource Sharing (CORS) simple headers before proceeding with a <code>PPB_Flash.Navigate</code> operation, which might allow remote attackers to bypass intended CORS restrictions via an inappropriate header. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6667 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.146 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6668 | None | None | Multiple unspecified vulnerabilities in Google V8 before 3.24.35.10, as used in Google Chrome before 33.0.1750.146, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1700 | None | None | Use-after-free vulnerability in <code>modules/speech/SpeechSynthesis.cpp</code> in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of a certain utterance data structure.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1701 | None | None | The <code>GenerateFunction</code> function in <code>bindings/scripts/code_generator_v8.pm</code> in Blink, as used in Google Chrome before 33.0.1750.149, does not implement a certain cross-origin restriction for the <code>EventTarget::dispatchEvent</code> function, which allows remote attackers to conduct Universal XSS (UXSS) attacks via vectors involving events.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1702 | None | None | Use-after-free vulnerability in the DatabaseThread::cleanupDatabaseThread function in modules/webdatabase/DatabaseThread.cpp in the web database implementation in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of scheduled tasks during shutdown of a thread.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1703 | None | None | Use-after-free vulnerability in the WebSocketDispatcherHost::SendOrDrop function in content/browser/renderer_host/websocket_dispatcher_host.cc in the Web Sockets implementation in Google Chrome before 33.0.1750.149 might allow remote attackers to bypass the sandbox protection mechanism by leveraging an incorrect deletion in a certain failure case.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1704 | None | None | Multiple unspecified vulnerabilities in Google V8 before 3.23.17.18, as used in Google Chrome before 33.0.1750.149, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1705 | None | None | Google V8, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1706 | None | None | crash in Google Chrome OS before 33.0.1750.152 allows attackers to inject commands via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1707 | None | None | Directory traversal vulnerability in CrosDisks in Google Chrome OS before 33.0.1750.152 has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1708 | None | None | The boot implementation in Google Chrome OS before 33.0.1750.152 does not properly consider file persistence, which allows remote attackers to execute arbitrary code via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1710 | None | None | The AsyncPixelTransfersCompletedQuery::End function in gpu/command_buffer/service/query_manager.cc in Google Chrome, as used in Google Chrome OS before 33.0.1750.152, does not check whether a certain position is within the bounds of a shared-memory segment, which allows remote attackers to cause a denial of service (GPU command-buffer memory corruption) or possibly have unspecified other impact via unknown vectors. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1711 | None | None | The GPU driver in the kernel in Google Chrome OS before 33.0.1750.152 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1713 | None | None | Use-after-free vulnerability in the AttributeSet function in bindings/templates/attributes.cpp in the bindings in Blink, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the document.location value.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1714 | None | None | The ScopedClipboardWriter::WritePickledData function in ui/base/clipboard/scoped_clipboard_write_r.cc in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows does not verify a certain format value, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the clipboard. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1715 | None | None | Directory traversal vulnerability in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows has unspecified impact and attack vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1716 | None | None | Cross-site scripting (XSS) vulnerability in the Runtime_SetPrototype function in runtime.cc in Google V8, as used in Google Chrome before 34.0.1847.116, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Universal XSS (UXSS)."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1717 | None | None | Google V8, as used in Google Chrome before 34.0.1847.116, does not properly use numeric casts during handling of typed arrays, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JavaScript code.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1718 | None | None | Integer overflow in the SoftwareFrameManager::SwapToNewFrame function in content/browser/renderer_host/software_frame_manager.cc in the software compositor in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted mapping of a large amount of renderer memory. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1719 | None | None | Use-after-free vulnerability in the WebSharedWorkerStub::OnTerminateWorkerContext function in content/worker/websharedworker_stub.cc in the Web Workers implementation in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger a SharedWorker termination during script loading. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1720 | None | None | Use-after-free vulnerability in the HTMLBodyElement::insertedInto function in core/html/HTMLBodyElement.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attributes.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1721 | None | None | Google V8, as used in Google Chrome before 34.0.1847.116, does not properly implement lazy deoptimization, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by improper handling of a heap allocation of a number outside the Small Integer (aka smi) range.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1722 | None | None | Use-after-free vulnerability in the RenderBlock::addChildIgnoringAnonymousColumnBlocks function in core/rendering/RenderBlock.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving addition of a child node.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1723 | None | None | The UnescapeURLWithOffsetsImpl function in net/base/escape.cc in Google Chrome before 34.0.1847.116 does not properly handle bidirectional Internationalized Resource Identifiers (IRIs), which makes it easier for remote attackers to spoof URLs via crafted use of right-to-left (RTL) Unicode text.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1724 | None | None | Use-after-free vulnerability in Free(b)soft Laboratory Speech Dispatcher 0.7.1, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service (application hang) or possibly have unspecified other impact via a text-to-speech request.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1725 | None | None | The base64DecodeInternal function in wtf/text/Base64.cpp in Blink, as used in Google Chrome before 34.0.1847.116, does not properly handle string data composed exclusively of whitespace characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via a window.atob method call.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1726 | None | None | The drag implementation in Google Chrome before 34.0.1847.116 allows user-assisted remote attackers to bypass the Same Origin Policy and forge local pathnames by leveraging renderer access.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1727 | None | None | Use-after-free vulnerability in content/renderer/renderer_webcolorchooser_impl.h in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to forms.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1728 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1729 | None | None | Multiple unspecified vulnerabilities in Google V8 before 3.24.35.22, as used in Google Chrome before 34.0.1847.116, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1730 | None | None | Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly store internationalization metadata, which allows remote attackers to bypass intended access restrictions by leveraging "type confusion" and reading property values, related to i18n.js and runtime.cc.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1731 | None | None | core/html/HTMLSelectElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly check renderer state upon a focus event, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion" for SELECT elements. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1732 | None | None | Use-after-free vulnerability in browser/ui/views/speech_recognition_bubble_views.cc in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via an INPUT element that triggers the presence of a Speech Recognition Bubble window for an incorrect duration. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1733 | None | None | The PointerCompare function in codegen.cc in Seccomp-BPF, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly merge blocks, which might allow remote attackers to bypass intended sandbox restrictions by leveraging renderer access.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1734 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1735 | None | None | Multiple unspecified vulnerabilities in Google V8 before 3.24.35.33, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1736 | None | None | Integer overflow in api.cc in Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1740 | None | None | Multiple use-after-free vulnerabilities in net/websockets/websocket_job.cc in the WebSockets implementation in Google Chrome before 34.0.1847.137 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to WebSocketJob deletion.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1741 | None | None | Multiple integer overflows in the replace-data functionality in the CharacterData interface implementation in core/dom/CharacterData.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to ranges.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1742 | None | None | Use-after-free vulnerability in the FrameSelection::updateAppearance function in core/editing/FrameSelection.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper RenderObject handling.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1743 | None | None | Use-after-free vulnerability in the StyleElement::removedFromDocument function in core/dom/StyleElement.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that triggers tree mutation. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1744 | None | None | Integer overflow in the AudioInputRendererHost::OnCreateStream function in content/browser/renderer_host/media/audio_input_renderer_host.cc in Google Chrome before 35.0.1916.114 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large shared-memory allocation.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1745 | None | None | Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger removal of an SVGFontFaceElement object, related to core/svg/SVGFontFaceElement.cpp.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1746 | None | None | The InMemoryUrlProtocol::Read function in media/filters/in_memory_url_protocol.cc in Google Chrome before 35.0.1916.114 relies on an insufficiently large integer data type, which allows remote attackers to cause a denial of service (out-of-bounds read) via vectors that trigger use of a large buffer.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1747 | None | None | Cross-site scripting (XSS) vulnerability in the DocumentLoader::maybeCreateArchive function in core/loader/DocumentLoader.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to inject arbitrary web script or HTML via crafted MHTML content, aka "Universal XSS (UXSS)."                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1748 | None | None | The ScrollView::paint function in platform/scroll/ScrollView.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to spoof the UI by extending scrollbar painting into the parent frame.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1749 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 35.0.1916.114 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3152 | None | None | Integer underflow in the LCodeGen::PrepareKeyedO perand function in arm/lithium-codegen-arm.cc in Google V8 before 3.25.28.16, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a negative key value.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3803 | None | None | The SpeechInput feature in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to enable microphone access and obtain speech-recognition text without indication via an INPUT element with a -x-webkit-speech attribute.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3154 | None | None | Use-after-free vulnerability in the ChildThread::Shutdown function in content/child/child_thread.cc in the filesystem API in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to a Blink shutdown.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3155 | None | None | net/spdy/spdy_write_queue.cc in the SPDY implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging incorrect queue maintenance.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3156 | None | None | Buffer overflow in the clipboard implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unexpected bitmap data, related to content/renderer/renderer_clipboard_client.cc and content/renderer/webclipboard_impl.cc.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3157 | None | None | Heap-based buffer overflow in the FFmpegVideoDecoder::GetVideoBuffer function in media/filters/ffmpeg_video_decoder.cc in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging VideoFrame data structures that are too small for proper interaction with an underlying FFmpeg library. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3159 | None | None | The WebContentsDelegateAndroid::OpenURLFromTab function in components/web_contents_delegate_android/web_contents_delegate_android.cc in Google Chrome before 36.0.1985.122 on Android does not properly restrict URL loading, which allows remote attackers to spoof the URL in the Omnibox via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3160 | None | None | The ResourceFetcher::canRequest function in core/fetch/ResourceFetcher.cpp in Blink, as used in Google Chrome before 36.0.1985.125, does not properly restrict subresource requests associated with SVG files, which allows remote attackers to bypass the Same Origin Policy via a crafted file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3161 | None | None | The WebMediaPlayerAndroid::load function in content/renderer/media/android/webmediaplayer_android.cc in Google Chrome before 36.0.1985.122 on Android does not properly interact with redirects, which allows remote attackers to bypass the Same Origin Policy via a crafted web site that hosts a video stream.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3162 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.125 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3165 | None | None | Use-after-free vulnerability in modules/websockets/WorkerThreadableWebSocketChannel.cpp in the Web Sockets implementation in Blink, as used in Google Chrome before 36.0.1985.143, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an unexpectedly long lifetime of a temporary object during method completion. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3166 | None | None | The Public Key Pinning (PKP) implementation in Google Chrome before 36.0.1985.143 on Windows, OS X, and Linux, and before 36.0.1985.135 on Android, does not correctly consider the properties of SPDY connections, which allows remote attackers to obtain sensitive information by leveraging the use of multiple domain names.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3167 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.143 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3168 | None | None | Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper caching associated with animation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3169 | None | None | Use-after-free vulnerability in core/dom/ContainerNode.cpp in the DOM implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging script execution that occurs before notification of node removal.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3170 | None | None | extensions/common/url_pattern.cc in Google Chrome before 37.0.2062.94 does not prevent use of a '\0' character in a host name, which allows remote attackers to spoof the extension permission dialog by relying on truncation after this character.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3171 | None | None | Use-after-free vulnerability in the V8 bindings in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper use of HashMap add operations instead of HashMap set operations, related to bindings/core/v8/DOMWrapperMap.h and bindings/core/v8/SerializedScriptValue.cpp.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3172 | None | None | The Debugger extension API in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 37.0.2062.94 does not validate a tab's URL before an attach operation, which allows remote attackers to bypass intended access limitations via an extension that uses a restricted URL, as demonstrated by a chrome:// URL.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3173 | None | None | The WebGL implementation in Google Chrome before 37.0.2062.94 does not ensure that clear calls interact properly with the state of a draw buffer, which allows remote attackers to cause a denial of service (read of uninitialized memory) via a crafted CANVAS element, related to gpu/command_buffer/service/framebuffer_manager.cc and gpu/command_buffer/service/gles2_cmd_decoder.cc. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3174 | None | None | modules/webaudio/BiquadDSPKernel.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 37.0.2062.94, does not properly consider concurrent threads during attempts to update biquad filter coefficients, which allows remote attackers to cause a denial of service (read of uninitialized memory) via crafted API calls.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3175 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors, related to the load_truetype_glyph function in truetype/ttgload.c in FreeType and other functions in other components.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3176 | None | None | Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3177.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3177 | None | None | Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3176.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3178 | None | None | Use-after-free vulnerability in core/dom/Node.cpp in Blink, as used in Google Chrome before 37.0.2062.120, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of render-tree inconsistencies.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3179 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.120 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-1568 | None | None | Mozilla Network Security Services (NSS) before 3.16.2.1, 3.16.x before 3.16.5, and 3.17.x before 3.17.1, as used in Mozilla Firefox before 32.0.3, Mozilla Firefox ESR 24.x before 24.8.1 and 31.x before 31.1.1, Mozilla Thunderbird before 24.8.1 and 31.x before 31.1.2, Mozilla SeaMonkey before 2.29.1, Google Chrome before 37.0.2062.124 on Windows and OS X, and Google Chrome OS before 37.0.2062.120, does not properly parse ASN.1 values in X.509 certificates, which makes it easier for remote attackers to spoof RSA signatures via a crafted certificate, aka a "signature malleability" issue. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3187 | None | None | Google Chrome before 37.0.2062.60 and 38.x before 38.0.2125.59 on iOS does not properly restrict processing of (1) facetime:// and (2) facetime-audio:// URLs, which allows remote attackers to obtain video and audio data from a device via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3188 | None | None | Google Chrome before 38.0.2125.101 and Chrome OS before 38.0.2125.101 do not properly handle the interaction of IPC and Google V8, which allows remote attackers to execute arbitrary code via vectors involving JSON data, related to improper parsing of an escaped index by ParseJsonObject in json-parser.h.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3189 | None | None | The chrome_pdf::CopyImage function in pdf/draw_utils.cc in the PDFium component in Google Chrome before 38.0.2125.101 does not properly validate image-data dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3190 | None | None | Use-after-free vulnerability in the Event::currentTarget function in core/events/Event.cpp in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that accesses the path property of an Event object.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3191 | None | None | Use-after-free vulnerability in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers a widget-position update that improperly interacts with the render tree, related to the FrameView::updateLayoutAndStyleForPainting function in core/frame/FrameView.cpp and the RenderLayerScrollableArea::setScrollOffset function in core/rendering/RenderLayerScrollableArea.cpp. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3192 | None | None | Use-after-free vulnerability in the ProcessingInstruction::setXSLStyleSheet function in core/dom/ProcessingInstruction.cpp in the DOM implementation in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3193 | None | None | The SessionService::GetLastSession function in browser/sessions/session_service.cc in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors that leverage "type confusion" for callback processing.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3194 | None | None | Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3195 | None | None | Google V8, as used in Google Chrome before 38.0.2125.101, does not properly track JavaScript heap-memory allocations as allocations of uninitialized memory and does not properly concatenate arrays of double-precision floating-point numbers, which allows remote attackers to obtain sensitive information via crafted JavaScript code, related to the PagedSpace::AllocateRaw and NewSpace::AllocateRaw functions in heap/spaces-inl.h, the LargeObjectSpace::AllocateRaw function in heap/spaces.cc, and the Runtime_ArrayConcat function in runtime.cc. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3196 | None | None | base/memory/shared_memory_win.cc in Google Chrome before 38.0.2125.101 on Windows does not properly implement read-only restrictions on shared memory, which allows attackers to bypass a sandbox protection mechanism via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3197 | None | None | The NavigationScheduler::schedulePageBlock function in core/loader/NavigationScheduler.cpp in Blink, as used in Google Chrome before 38.0.2125.101, does not properly provide substitute data for pages blocked by the XSS auditor, which allows remote attackers to obtain sensitive information via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3198 | None | None | The Instance::HandleInputEvent function in pdf/instance.cc in the PDFium component in Google Chrome before 38.0.2125.101 interprets a certain -1 value as an index instead of a no-visible-page error code, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3199 | None | None | The wrap function in bindings/core/v8/custom/V8EventCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 38.0.2125.101, has an erroneous fallback outcome for wrapper-selection failures, which allows remote attackers to cause a denial of service via vectors that trigger stopping a worker process that had been handling an Event object. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3200 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 38.0.2125.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7967 | None | None | Multiple unspecified vulnerabilities in Google V8 before 3.28.71.15, as used in Google Chrome before 38.0.2125.101, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3201 | None | None | core/rendering/compositing/RenderLayerCompositor.cpp in Blink, as used in Google Chrome before 38.0.2125.102 on Android, does not properly handle a certain IFRAME overflow condition, which allows remote attackers to spoof content via a crafted web site that interferes with the scrollbar.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7899 | None | None | Google Chrome before 38.0.2125.101 allows remote attackers to spoof the address bar by placing a blob: substring at the beginning of the URL, followed by the original URI scheme and a long username string.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7900 | None | None | Use-after-free vulnerability in the CPDF_Parser::IsLinearizedFile function in fpdfapi/fpdf_parser/fpdf_parser_parser.cpp in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7901 | None | None | Integer overflow in the opj_t2_read_packet_data function in fxcodec/fx_libopenjpeg/libopenjpeg20/t2.c in OpenJPEG in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long segment in a JPEG image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7902 | None | None | Use-after-free vulnerability in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7903 | None | None | Buffer overflow in OpenJPEG before r2911 in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JPEG image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7904 | None | None | Buffer overflow in Skia, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7905 | None | None | Google Chrome before 39.0.2171.65 on Android does not prevent navigation to a URL in cases where an intent for the URL lacks CATEGORY_BROWSABLE, which allows remote attackers to bypass intended access restrictions via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7906 | None | None | Use-after-free vulnerability in the Pepper plugins in Google Chrome before 39.0.2171.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Flash content that triggers an attempted PepperMediaDeviceManager access outside of the object's lifetime.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7907 | None | None | Multiple use-after-free vulnerabilities in modules/screen_orientation/ScreenOrientationController.cpp in Blink, as used in Google Chrome before 39.0.2171.65, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger improper handling of a detached frame, related to the (1) lock and (2) unlock methods. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7908 | None | None | Multiple integer overflows in the CheckMov function in media/base/container_names.cc in Google Chrome before 39.0.2171.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a large atom in (1) MPEG-4 or (2) QuickTime .mov data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7909 | None | None | effects/SkDashPathEffect.cpp in Skia, as used in Google Chrome before 39.0.2171.65, computes a hash key using uninitialized integer values, which might allow remote attackers to cause a denial of service by rendering crafted data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7910 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 39.0.2171.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1793 | None | None | rendering/svg/RenderSVGResourceFilter.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted SVG document that leads to a "stale pointer."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1794 | None | None | Integer overflow in the FilterEffect::copyImageBytes function in platform/graphics/filters/FilterEffect.cpp in the SVG filter implementation in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted dimensions.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1795 | None | None | Integer underflow in the HTMLFormElement::removeFormElement function in html/HTMLFormElement.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document containing a FORM element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1796 | None | None | Use-after-free vulnerability in the FrameView::calculateScrollbarModesForLayout function in page/FrameView.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that calls the removeChild method during interaction with a FRAME element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1798 | None | None | rendering/svg/RenderSVGText.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 does not properly perform a cast of an unspecified variable during an attempt to handle a block child, which allows remote attackers to cause a denial of service (application crash) or possibly have unknown other impact via a crafted text element in an SVG document.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7923 | None | None | The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a look-behind expression.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7924 | None | None | Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering duplicate BLOB references, related to content/browser/indexed_db/indexed_db_callbacks.cc and content/browser/indexed_db/indexed_db_dispatcher_host.cc.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7925 | None | None | Use-after-free vulnerability in the WebAudio implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an audio-rendering thread in which AudioNode data is improperly maintained.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7926 | None | None | The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a zero-length quantifier.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7927 | None | None | The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7928 | None | None | hydrogen.cc in Google V8, as used Google Chrome before 40.0.2214.91, does not properly handle arrays with holes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers an array copy.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7929 | None | None | Use-after-free vulnerability in the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving movement of a SCRIPT element across documents. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7930 | None | None | Use-after-free vulnerability in core/events/TreeScopeEventContext.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of TreeScope data.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7931 | None | None | factory.cc in Google V8, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of backing-store pointers.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7932 | None | None | Use-after-free vulnerability in the Element::detach function in core/dom/Element.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving pending updates of detached elements.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7933 | None | None | Use-after-free vulnerability in the matroska_read_seek function in libavformat/matroskadec.c in FFmpeg before 2.5.1, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska file that triggers improper maintenance of tracks data. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7934 | None | None | Use-after-free vulnerability in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unexpected absence of document data structures.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7935 | None | None | Use-after-free vulnerability in browser/speech/tts_message_filter.cc in the Speech implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving utterances from a closed tab.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7936 | None | None | Use-after-free vulnerability in the ZoomBubbleView::Close function in browser/ui/views/location_bar/zoom_bubble_view.cc in the Views implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that triggers improper maintenance of a zoom bubble. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7937 | None | None | Multiple off-by-one errors in libavcodec/vorbisdec.c in FFmpeg before 2.4.2, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Vorbis I data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7938 | None | None | The Fonts implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7939 | None | None | Google Chrome before 40.0.2214.91, when the Harmony proxy in Google V8 is enabled, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code with Proxy.create and console.log calls, related to HTTP responses that lack an "X-Content-Type-Options: nosniff" header.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7940 | None | None | The collator implementation in i18n/ucol.cpp in International Components for Unicode (ICU) 52 through SVN revision 293126, as used in Google Chrome before 40.0.2214.91, does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted character sequence.    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7941 | None | None | The SelectionOwner::ProcessTarget function in ui/base/x/selection_owner.cc in the UI implementation in Google Chrome before 40.0.2214.91 uses an incorrect data type for a certain length value, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted X11 data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7942 | None | None | The Fonts implementation in Google Chrome before 40.0.2214.91 does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7943 | None | None | Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7944 | None | None | The sycc422_to_rgb function in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 40.0.2214.91, does not properly handle odd values of image width, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7945 | None | None | OpenJPEG before r2908, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, and t2.c.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7946 | None | None | The RenderTable::simplifiedNormalFlowLayout function in core/rendering/RenderTable.cpp in Blink, as used in Google Chrome before 40.0.2214.91, skips captions during table layout in certain situations, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors related to the Fonts implementation.     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7947 | None | None | OpenJPEG before r2944, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, pi.c, t1.c, t2.c, and tcd.c.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-7948 | None | None | The AppCacheUpdateJob::URLFetcher::OnResponseStarted function in content/browser/appcache/appcache_update_job.cc in Google Chrome before 40.0.2214.91 proceeds with AppCache caching for SSL sessions even if there is an X.509 certificate error, which allows man-in-the-middle attackers to spoof HTML5 application content via a crafted certificate. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1205 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.91 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1346 | None | None | Multiple unspecified vulnerabilities in Google V8 before 3.30.33.15, as used in Google Chrome before 40.0.2214.91, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-9646 | None | None | Unquoted Windows search path vulnerability in the GoogleChromeDistribution::DoPostUninstallOperations function in installer/util/google_chrome_distribution.cc in the uninstall-survey feature in Google Chrome before 40.0.2214.91 allows local users to gain privileges via a Trojan horse program in the %SYSTEMDRIVE% directory, as demonstrated by program.exe, a different vulnerability than CVE-2015-1205.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-9647 | None | None | Use-after-free vulnerability in PDFium, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/src/fpdfview.cpp and fpdfsdk/src/fsdk_mgr.cpp, a different vulnerability than CVE-2015-1205.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-9648 | None | None | components/navigation_interception/intercept_navigation_resource_throttle.cc in Google Chrome before 40.0.2214.91 on Android does not properly restrict use of intent: URLs to open an application after navigation to a web site, which allows remote attackers to cause a denial of service (loss of browser access to that site) via crafted JavaScript code, as demonstrated by pandora.com and the Pandora application, a different vulnerability than CVE-2015-1205. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1359 | None | None | Multiple off-by-one errors in fpdfapi/fpdf_font/font_int.h in PDFium, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted PDF document, related to an "intra-object-overflow" issue, a different vulnerability than CVE-2015-1205.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1360 | None | None | Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data that is improperly handled during text drawing, related to gpu/GrBitmapTextContext.cpp and gpu/GrDistanceFieldTextContext.cpp, a different vulnerability than CVE-2015-1205.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1361 | None | None | platform/image-decoders/ImageFrame.h in Blink, as used in Google Chrome before 40.0.2214.91, does not initialize a variable that is used in calls to the Skia SkBitmap::setAlphaType function, which might allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document, a different vulnerability than CVE-2015-1205.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1209 | None | None | Use-after-free vulnerability in the VisibleSelection::nonBoundaryShadowTreeRootNode function in core/editing/VisibleSelection.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers improper handling of a shadow-root anchor. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1210 | None | None | The V8ThrowException::createDOMException function in bindings/core/v8/V8ThrowException.cpp in the V8 bindings in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, does not properly consider frame access restrictions during the throwing of an exception, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1211 | None | None | The OriginCanAccessServiceWorkers function in content/browser/service_worker/service_worker_dispatcher_host.cc in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android does not properly restrict the URI scheme during a ServiceWorker registration, which allows remote attackers to gain privileges via a filesystem: URI.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1212 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-5319 | None | None | content/renderer/device_sensors/device_motion_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate accelerometer data, which makes it easier for remote attackers to capture keystrokes via a crafted web site that listens for ondevicemotion events, a different vulnerability than CVE-2015-1231.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-9689 | None | None | content/renderer/device_sensors/device_orientation_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate gyroscope data, which makes it easier for remote attackers to obtain speech signals from a device's physical environment via a crafted web site that listens for ondeviceorientation events, a different vulnerability than CVE-2015-1231.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1213 | None | None | The SkBitmap::ReadRawPixels function in core/SkBitmap.cpp in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1214 | None | None | Integer overflow in the SkAutoSTArray implementation in include/core/SkTemplates.h in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a reset action with a large count value, leading to an out-of-bounds write operation.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1215 | None | None | The filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1216 | None | None | Use-after-free vulnerability in the V8Window::namedPropertyGetterCustom function in bindings/core/v8/custom/V8WindowCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a frame detachment.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1217 | None | None | The V8LazyEventListener::prepareListenerObject function in bindings/core/v8/V8LazyEventListener.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, does not properly compile listeners, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1218 | None | None | Multiple use-after-free vulnerabilities in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger movement of a SCRIPT element to different documents, related to (1) the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp and (2) the SVGScriptElement::didMoveToNewDocument function in core/svg/SVGScriptElement.cpp. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1219 | None | None | Integer overflow in the SkMallocPixelRef::NewAllocate function in core/SkMallocPixelRef.cpp in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted allocation of a large amount of memory during WebGL rendering.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1220 | None | None | Use-after-free vulnerability in the GIFImageReader::parseData function in platform/image-decoders/gif/GIFImageReader.cpp in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted frame size in a GIF image.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1221 | None | None | Use-after-free vulnerability in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect ordering of operations in the Web SQL Database thread relative to Blink's main thread, related to the shutdown function in web/WebKit.cpp.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1222 | None | None | Multiple use-after-free vulnerabilities in the ServiceWorkerScriptCacheMap implementation in content/browser/service_worker/service_worker_script_cache_map.cc in Google Chrome before 41.0.2272.76 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a ServiceWorkerContextWrapper::DeleteAndStartOver call, related to the NotifyStartedCaching and NotifyFinishedCaching functions. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1223 | None | None | Multiple use-after-free vulnerabilities in core/html/HTMLInputElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger extraneous change events, as demonstrated by events for invalid input or input to read-only fields, related to the initializeTypeInParsing and updateType functions.     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1224 | None | None | The VpxVideoDecoder::VpxDecode function in media/filters/vpx_video_decoder.cc in the vpxdecoder implementation in Google Chrome before 41.0.2272.76 does not ensure that alpha-plane dimensions are identical to image dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted VPx video data.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1225 | None | None | PDFium, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1226 | None | None | The DebuggerFunction::InitAgentHost function in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 41.0.2272.76 does not properly restrict what URLs are available as debugger targets, which allows remote attackers to bypass intended access restrictions via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1227 | None | None | The DragImage::create function in platform/DragImage.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not initialize memory for image drawing, which allows remote attackers to have an unspecified impact by triggering a failed image decoding, as demonstrated by an image for which the default orientation cannot be used.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1228 | None | None | The RenderCounter::updateCounter function in core/rendering/RenderCounter.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not force a relayout operation and consequently does not initialize memory for a data structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted Cascading Style Sheets (CSS) token sequence. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1229 | None | None | net/http/proxy_client_socket.cc in Google Chrome before 41.0.2272.76 does not properly handle a 407 (aka Proxy Authentication Required) HTTP status code accompanied by a Set-Cookie header, which allows remote proxy servers to conduct cookie-injection attacks via a crafted response.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1230 | None | None | The getHiddenProperty function in bindings/core/v8/V8EventListenerList.h in Blink, as used in Google Chrome before 41.0.2272.76, has a name conflict with the AudioContext class, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that adds an AudioContext event listener and triggers "type confusion."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1231 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 41.0.2272.76 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1232 | None | None | Array index error in the MidiManagerUsb::DispatchSendMidiData function in media/midi/midi_manager_usb.cc in Google Chrome before 41.0.2272.76 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging renderer access to provide an invalid port index that triggers an out-of-bounds write operation, a different vulnerability than CVE-2015-1212.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-2238 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.1.0.21, as used in Google Chrome before 41.0.2272.76, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-2239 | None | None | Google Chrome before 41.0.2272.76, when Instant Extended mode is used, does not properly consider the interaction between the "1993 search" features and restore-from-disk RELOAD transitions, which makes it easier for remote attackers to spoof the address bar for a search-results page by leveraging (1) a compromised search engine or (2) an XSS vulnerability in a search engine, a different vulnerability than CVE-2015-1231. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1233 | None | None | Google Chrome before 41.0.2272.118 does not properly handle the interaction of IPC, the Gamepad API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1234 | None | None | Race condition in gpu/command_buffer/service/gles2_cmd_decoder.cc in Google Chrome before 41.0.2272.118 allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact by manipulating OpenGL ES commands.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1235 | None | None | The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in the HTML parser in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy via a crafted HTML document with an IFRAME element.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1236 | None | None | The MediaElementAudioSourceNode::process function in modules/webaudio/MediaElementAudioSourceNode.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy and obtain sensitive audio sample values via a crafted web site containing a media element.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1237 | None | None | Use-after-free vulnerability in the <code>RenderFrameImpl::OnMessageReceived</code> function in <code>content/renderer/render_frame_impl.cc</code> in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger renderer IPC messages during a detach operation.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1238 | None | None | Skia, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1240 | None | None | <code>gpu/blink/webgraphicscontext3d_impl.cc</code> in the WebGL implementation in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebGL program that triggers a state inconsistency.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1241 | None | None | Google Chrome before 42.0.2311.90 does not properly consider the interaction of page navigation with the handling of touch events and gesture events, which allows remote attackers to trigger unintended UI actions via a crafted web site that conducts a "tapjacking" attack.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1242 | None | None | The <code>ReduceTransitionElementsKind</code> function in <code>hydrogen-check-elimination.cc</code> in Google V8 before 4.2.77.8, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that leverages "type confusion" in the check-elimination optimization.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1244 | None | None | The <code>URLRequest::GetHSTSRedirect</code> function in <code>url_request/url_request.cc</code> in Google Chrome before 42.0.2311.90 does not replace the <code>ws</code> scheme with the <code>wss</code> scheme whenever an HSTS Policy is active, which makes it easier for remote attackers to obtain sensitive information by sniffing the network for WebSocket traffic.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1245 | None | None | Use-after-free vulnerability in the <code>OpenPDFInReaderView::Update</code> function in <code>browser/ui/views/location_bar/open_pdf_in_reader_view.cc</code> in Google Chrome before 41.0.2272.76 might allow user-assisted remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering interaction with a PDFium "Open PDF in Reader" button that has an invalid tab association. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1246 | None | None | Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1247 | None | None | The SearchEngineTabHelper::OnPageHasOSDD function in browser/ui/search_engines/search_engine_tab_helper.cc in Google Chrome before 42.0.2311.90 does not prevent use of a file: URL for an OpenSearch descriptor XML document, which might allow remote attackers to obtain sensitive information from local files via a crafted (1) http or (2) https web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1248 | None | None | The FileSystem API in Google Chrome before 40.0.2214.91 allows remote attackers to bypass the SafeBrowsing for Executable Files protection mechanism by creating a .exe file in a temporary filesystem and then referencing this file with a filesystem:http: URL.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1249 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.90 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-3333 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.2.77.14, as used in Google Chrome before 42.0.2311.90, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-3334 | None | None | browser/ui/website_settings/website_settings.cc in Google Chrome before 42.0.2311.90 does not always display "Media: Allowed by you" in a Permissions table after the user has granted camera permission to a web site, which might make it easier for user-assisted remote attackers to obtain sensitive video data from a device's physical environment via a crafted web site that turns on the camera at a time when the user believes that camera access is prohibited. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-3335 | None | None | The NaClSandbox::InitializeLayerTwoSandbox function in components/nacl/loader/sandbox_linux/nacl_sandbox_linux.cc in Google Chrome before 42.0.2311.90 does not have RLIMIT_AS and RLIMIT_DATA limits for Native Client (aka NaCl) processes, which might make it easier for remote attackers to conduct row-hammer attacks or have unspecified other impact by leveraging the ability to run a crafted program in the NaCl sandbox.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-3336 | None | None | Google Chrome before 42.0.2311.90 does not always ask the user before proceeding with CONTENT_SETTINGS_TYPE_FULLSCREEN and CONTENT_SETTINGS_TYPE_MOUSELOCK changes, which allows user-assisted remote attackers to cause a denial of service (UI disruption) by constructing a crafted HTML document containing JavaScript code with requestFullScreen and requestPointerLock calls, and arranging for the user to access this document with a file: URL. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1243 | None | None | Use-after-free vulnerability in the MutationObserver::disconnect function in core/dom/MutationObserver.cpp in the DOM implementation in Blink, as used in Google Chrome before 42.0.2311.135, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an attempt to unregister a MutationObserver object that is not currently registered.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1250 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.135 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1251 | None | None | Use-after-free vulnerability in the SpeechRecognitionClient implementation in the Speech subsystem in Google Chrome before 43.0.2357.65 allows remote attackers to execute arbitrary code via a crafted document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1252 | None | None | common/partial_circular_buffer.cc in Google Chrome before 43.0.2357.65 does not properly handle wraps, which allows remote attackers to bypass a sandbox protection mechanism or cause a denial of service (out-of-bounds write) via vectors that trigger a write operation with a large amount of data, related to the PartialCircularBuffer::Write and PartialCircularBuffer::DoWrite functions.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1253 | None | None | core/html/parser/HTMLConstructionSite.cpp in the DOM implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that appends a child to a SCRIPT element, related to the insert and executeReparentTask functions.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1254 | None | None | core/dom/Document.cpp in Blink, as used in Google Chrome before 43.0.2357.65, enables the inheritance of the designMode attribute, which allows remote attackers to bypass the Same Origin Policy by leveraging the availability of editing.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1255 | None | None | Use-after-free vulnerability in content/renderer/media/webaudio_capturer_source.c in the WebAudio implementation in Google Chrome before 43.0.2357.65 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging improper handling of a stop action for an audio track.                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1256 | None | None | Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that leverages improper handling of a shadow tree for a use element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1257 | None | None | platform/graphics/filters/FIColorMatrix.cpp in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, does not properly handle an insufficient number of values in an feColorMatrix filter, which allows remote attackers to cause a denial of service (container overflow) or possibly have unspecified other impact via a crafted document. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1258 | None | None | Google Chrome before 43.0.2357.65 relies on libvpx code that was not built with an appropriate --size-limit value, which allows remote attackers to trigger a negative value for a size field, and consequently cause a denial of service or possibly have unspecified other impact, via a crafted frame size in VP9 video data.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1259 | None | None | PDFium, as used in Google Chrome before 43.0.2357.65, does not properly initialize memory, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1260 | None | None | Multiple use-after-free vulnerabilities in content/renderer/media/user_media_client_impl.cc in the WebRTC implementation in Google Chrome before 43.0.2357.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that executes upon completion of a getUserMedia request.                      |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1261 | None | None | android/java/src/org/chromium/chrome/browser/Web<br>siteSettingsPopup.java in Google Chrome before<br>43.0.2357.65 on Android does not properly restrict<br>use of a URL's fragment identifier during<br>construction of a page-info popup, which allows<br>remote attackers to spoof the URL bar or deliver<br>misleading popup content via crafted text.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1262 | None | None | platform/fonts/shaping/HarfBuzzShaper.cpp in Blink,<br>as used in Google Chrome before 43.0.2357.65,<br>does not initialize a certain width field, which allows<br>remote attackers to cause a denial of service or<br>possibly have unspecified other impact via crafted<br>Unicode text.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1263 | None | None | The Spellcheck API implementation in Google<br>Chrome before 43.0.2357.65 does not use an<br>HTTPS session for downloading a Hunspell<br>dictionary, which allows man-in-the-middle attackers<br>to deliver incorrect spelling suggestions or possibly<br>have unspecified other impact via a crafted file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1264 | None | None | Cross-site scripting (XSS) vulnerability in Google<br>Chrome before 43.0.2357.65 allows user-assisted<br>remote attackers to inject arbitrary web script or<br>HTML via crafted data that is improperly handled by<br>the Bookmarks feature.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1265 | None | None | Multiple unspecified vulnerabilities in Google<br>Chrome before 43.0.2357.65 allow attackers to<br>cause a denial of service or possibly have other<br>impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-3910 | None | None | Multiple unspecified vulnerabilities in Google V8<br>before 4.3.61.21, as used in Google Chrome before<br>43.0.2357.65, allow attackers to cause a denial of<br>service or possibly have other impact via unknown<br>vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1266 | None | None | content/browser/webui/content_web_ui_controller_fa<br>ctory.cc in Google Chrome before 43.0.2357.130<br>does not properly consider the scheme in<br>determining whether a URL is associated with a<br>WebUI SiteInstance, which allows remote attackers<br>to bypass intended access restrictions via a similar<br>URL, as demonstrated by use of http://gpu when<br>there is a WebUI class for handling chrome://gpu<br>requests. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1267 | None | None | Blink, as used in Google Chrome before 43.0.2357.130, does not properly restrict the creation context during creation of a DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that uses a Blink public API, related to WebArrayBufferConverter.cpp, WebBlob.cpp, WebDOMError.cpp, and WebDOMFileSystem.cpp.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1268 | None | None | bindings/scripts/v8_types.py in Blink, as used in Google Chrome before 43.0.2357.130, does not properly select a creation context for a return value's DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code, as demonstrated by use of a data: URL.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1269 | None | None | The DecodeHSTSPreloadRaw function in net/http/transport_security_state.cc in Google Chrome before 43.0.2357.130 does not properly canonicalize DNS hostnames before making comparisons to HSTS or HPKP preload entries, which allows remote attackers to bypass intended access restrictions via a string that (1) ends in a . (dot) character or (2) is not entirely lowercase.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1270 | None | None | The ucnv_io_getConverterName function in common/ucnv_io.cpp in International Components for Unicode (ICU), as used in Google Chrome before 44.0.2403.89, mishandles converter names with initial x- substrings, which allows remote attackers to cause a denial of service (read of uninitialized memory) or possibly have unspecified other impact via a crafted file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1271 | None | None | PDFium, as used in Google Chrome before 44.0.2403.89, does not properly handle certain out-of-memory conditions, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted PDF document that triggers a large memory allocation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1272 | None | None | Use-after-free vulnerability in the GPU process implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the continued availability of a GPUChannelHost data structure during Blink shutdown, related to content/browser/gpu/browser_gpu_channel_host_factory.cc and content/renderer/render_thread_impl.cc. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1273 | None | None | Heap-based buffer overflow in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service or possibly have unspecified other impact via invalid JPEG2000 data in a PDF document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1274 | None | None | Google Chrome before 44.0.2403.89 does not ensure that the auto-open list omits all dangerous file types, which makes it easier for remote attackers to execute arbitrary code by providing a crafted file and leveraging a user's previous "Always open files of this type" choice, related to download_commands.cc and download_prefs.cc. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1275 | None | None | Cross-site scripting (XSS) vulnerability in org/chromium/chrome/browser/UrlUtilities.java in Google Chrome before 44.0.2403.89 on Android allows remote attackers to inject arbitrary web script or HTML via a crafted intent: URL, as demonstrated by a trailing alert(document.cookie);// substring, aka "Universal XSS (UXSS)."          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1276 | None | None | Use-after-free vulnerability in content/browser/indexed_db/indexed_db_backing_store.cc in the IndexedDB implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an abort action before a certain write operation.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1277 | None | None | Use-after-free vulnerability in the accessibility implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging lack of certain validity checks for accessibility-tree data structures.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1278 | None | None | content/browser/web_contents/web_contents_impl.cc in Google Chrome before 44.0.2403.89 does not ensure that a PDF document's modal dialog is closed upon navigation to an interstitial page, which allows remote attackers to spoof URLs via a crafted document, as demonstrated by the alert_dialog.pdf document.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1279 | None | None | Integer overflow in the CBig2_Image::expand function in fxcodec/jbig2/JBig2_Image.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via large height and stride values.                              |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1280 | None | None | SkPictureShader.cpp in Skia, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging access to a renderer process and providing crafted serialized data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1281 | None | None | core/loader/ImageLoader.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly determine the V8 context of a microtask, which allows remote attackers to bypass Content Security Policy (CSP) restrictions by providing an image from an unintended source.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1282 | None | None | Multiple use-after-free vulnerabilities in fpdfsdk/src/javascript/Document.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to the (1) Document::delay and (2) Document::DoFieldDelay functions.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1283 | None | None | Multiple integer overflows in the XML_GetBuffer function in Expat through 2.1.0, as used in Google Chrome before 44.0.2403.89 and other products, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted XML data, a related issue to CVE-2015-2716.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1284 | None | None | The LocalFrame::isURLAllowed function in core/frame/LocalFrame.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly check for a page's maximum number of frames, which allows remote attackers to cause a denial of service (invalid count value and use-after-free) or possibly have unspecified other impact via crafted JavaScript code that makes many createElement calls for IFRAME elements. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1285 | None | None | The XSSAuditor::canonicalize function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 44.0.2403.89, does not properly choose a truncation point, which makes it easier for remote attackers to obtain sensitive information via an unspecified linear-time attack.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1286 | None | None | Cross-site scripting (XSS) vulnerability in the V8ContextNativeHandler::GetModuleSystem function in extensions/renderer/v8_context_native_handler.cc in Google Chrome before 44.0.2403.89 allows remote attackers to inject arbitrary web script or HTML by leveraging the lack of a certain V8 context restriction, aka a Blink "Universal XSS (UXSS)."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1287 | None | None | Blink, as used in Google Chrome before 44.0.2403.89, enables a quirks-mode exception that limits the cases in which a Cascading Style Sheets (CSS) document is required to have the text/css content type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related to core/fetch/CSSStyleSheetResource.cpp.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1288 | None | None | The Spellcheck API implementation in Google Chrome before 44.0.2403.89 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file, a related issue to CVE-2015-1263.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1289 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 44.0.2403.89 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-5605 | None | None | The regular-expression implementation in Google V8, as used in Google Chrome before 44.0.2403.89, mishandles interrupts, which allows remote attackers to cause a denial of service (application crash) via crafted JavaScript code, as demonstrated by an error in garbage collection during allocation of a stack-overflow exception message.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-4491 | None | None | Integer overflow in the make_filter_table function in pixops/pixops.c in gdk-pixbuf before 2.31.5, as used in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 on Linux, Google Chrome on Linux, and other products, allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via crafted bitmap dimensions that are mishandled during scaling. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1291 | None | None | The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not check whether a node is expected, which allows remote attackers to bypass the Same Origin Policy or cause a denial of service (DOM tree corruption) via a web site with crafted JavaScript code and IFRAME elements.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1292 | None | None | The NavigatorServiceWorker::serviceWorker function in modules/serviceworkers/NavigatorServiceWorker.cpp in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy by accessing a Service Worker.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1293 | None | None | The DOM implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1294 | None | None | Use-after-free vulnerability in the SkMatrix::invertNonIdentity function in core/SkMatrix.cpp in Skia, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering the use of matrix elements that lead to an infinite result during an inversion calculation.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1295 | None | None | Multiple use-after-free vulnerabilities in the PrintWebViewHelper class in components/printing/renderer/print_web_view_helper.cc in Google Chrome before 45.0.2454.85 allow user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact by triggering nested IPC messages during preparation for printing, as demonstrated by messages associated with PDF documents in conjunction with messages about printer capabilities. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1296 | None | None | The UnescapeURLWithAdjustmentsImpl implementation in net/base/escape.cc in Google Chrome before 45.0.2454.85 does not prevent display of Unicode LOCK characters in the omnibox, which makes it easier for remote attackers to spoof the SSL lock icon by placing one of these characters at the end of a URL, as demonstrated by the omnibox in localizations for right-to-left languages.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1297 | None | None | The WebRequest API implementation in extensions/browser/api/web_request/web_request_api.cc in Google Chrome before 45.0.2454.85 does not properly consider a request's source before accepting the request, which allows remote attackers to bypass intended access restrictions via a crafted (1) app or (2) extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1298 | None | None | The RuntimeEventRouter::OnExtensionUninstalled function in extensions/browser/api/runtime/runtime_api.cc in Google Chrome before 45.0.2454.85 does not ensure that the setUninstallURL preference corresponds to the URL of a web site, which allows user-assisted remote attackers to trigger access to an arbitrary URL via a crafted extension that is uninstalled.          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1299 | None | None | Use-after-free vulnerability in the shared-timer implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging erroneous timer firing, related to ThreadTimers.cpp and Timer.cpp.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1300 | None | None | The FrameFetchContext::updateTimingInfoForIFrameNavigation function in core/loader/FrameFetchContext.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to obtain sensitive information via crafted JavaScript code that leverages a history.back call. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1301 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 45.0.2454.85 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6580 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.5.103.29, as used in Google Chrome before 45.0.2454.85, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6581 | None | None | Double free vulnerability in the opj_j2k_copy_default_tcp_and_create_tcd function in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6582 | None | None | The decompose function in platform/transforms/TransformationMatrix.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not verify that a matrix inversion succeeded, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted web site. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6583 | None | None | Google Chrome before 45.0.2454.85 does not display a location bar for a hosted app's window after navigation away from the installation site, which might make it easier for remote attackers to spoof content via a crafted app, related to browser.cc and hosted_app_browser_controller.cc.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1303 | None | None | bindings/core/v8/V8DOMWrapper.h in Blink, as used in Google Chrome before 45.0.2454.101, does not perform a rethrow action to propagate information about a cross-context exception, which allows remote attackers to bypass the Same Origin Policy via a crafted HTML document containing an IFRAME element.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1304 | None | None | object-observe.js in Google V8, as used in Google Chrome before 45.0.2454.101, does not properly restrict method calls on access-checked objects, which allows remote attackers to bypass the Same Origin Policy via a (1) observe or (2) getNotifier call.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6755 | None | None | The ContainerNode::parserInsertBefore function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 46.0.2490.71, proceeds with a DOM tree insertion in certain cases where a parent node no longer contains a child node, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6756 | None | None | Use-after-free vulnerability in the CPDFSDK_PageView implementation in fpdfsdk/src/fsdk_mgr.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging mishandling of a focused annotation in a PDF document.              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6757 | None | None | Use-after-free vulnerability in content/browser/service_worker/embedded_worker_instance.cc in the ServiceWorker implementation in Google Chrome before 46.0.2490.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging object destruction in a callback.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6758 | None | None | The CPDF_Document::GetPage function in fpdfapi/fpdf_parser/fpdf_parser_document.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, does not properly perform a cast of a dictionary object, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6759 | None | None | The shouldTreatAsUniqueOrigin function in platform/weborigin/SecurityOrigin.cpp in Blink, as used in Google Chrome before 46.0.2490.71, does not ensure that the origin of a LocalStorage resource is considered unique, which allows remote attackers to obtain sensitive information via vectors involving a blob: URL.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6760 | None | None | The Image11::map function in renderer/d3d/d3d11/Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write) or possibly have unspecified other impact via vectors involving a removed device.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6761 | None | None | The update_dimensions function in libavcodec/vp8.c in FFmpeg through 2.8.1, as used in Google Chrome before 46.0.2490.71 and other products, relies on a coefficient-partition count during multi-threaded operation, which allows remote attackers to cause a denial of service (race condition and memory corruption) or possibly have unspecified other impact via a crafted WebM file. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6762 | None | None | The CSSFontFaceSrcValue::fetch function in core/css/CSSFontFaceSrcValue.cpp in the Cascading Style Sheets (CSS) implementation in Blink, as used in Google Chrome before 46.0.2490.71, does not use the CORS cross-origin request algorithm when a font's URL appears to be a same-origin URL, which allows remote web servers to bypass the Same Origin Policy via a redirect.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6763 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 46.0.2490.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-7834 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.6.85.23, as used in Google Chrome before 46.0.2490.71, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |

|               |                    |               |          |      |  |
|---------------|--------------------|---------------|----------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1302 | None     | None | The PDF viewer in Google Chrome before 46.0.2490.86 does not properly restrict scripting messages and API exposure, which allows remote attackers to bypass the Same Origin Policy via an unintended embedder or unintended plugin loading, related to pdf.js and out_of_process_instance.cc.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6764 | CRITICAL | 9.8  | The BasicJsonStringifier::SerializeJSONArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6765 | None     | None | Use-after-free vulnerability in content/browser/appcache/appcache_update_job.cc in Google Chrome before 47.0.2526.73 allows remote attackers to execute arbitrary code or cause a denial of service by leveraging the mishandling of AppCache update jobs.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6766 | None     | None | Use-after-free vulnerability in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers with renderer access to cause a denial of service or possibly have unspecified other impact by leveraging incorrect AppCacheUpdateJob behavior associated with duplicate cache selection.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6767 | None     | None | Use-after-free vulnerability in content/browser/appcache/appcache_dispatcher_host.cc in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect pointer maintenance associated with certain callbacks.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6768 | None     | None | The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6770.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6769 | None     | None | The provisional-load commit implementation in WebKit/Source/bindings/core/v8/WindowProxy.cpp in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy by leveraging a delay in window proxy clearing.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6770 | None     | None | The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6768.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6771 | None | None | js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6772 | None | None | The DOM implementation in Blink, as used in Google Chrome before 47.0.2526.73, does not prevent javascript: URL navigation while a document is being detached, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that improperly interacts with a plugin.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6773 | None | None | The convolution implementation in Skia, as used in Google Chrome before 47.0.2526.73, does not properly constrain row lengths, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted graphics data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6774 | None | None | Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.c in the Extensions implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that modifies a pointer used for reporting loadTimes data.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6775 | None | None | fpdfsdk/src/jsapi/fixjs_v8.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, does not use signatures, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6776 | None | None | The opj_dwt_decode_1* functions in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 47.0.2526.73, allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during a discrete wavelet transform.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6777 | None | None | Use-after-free vulnerability in the ContainerNode::notifyNodeInsertedInternal function in WebKit/Source/core/dom/ContainerNode.cpp in the DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOMCharacterDataModified events for certain detached-subtree insertions. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6778 | None | None | The CJBIG2_SymbolDict class in fxcodec/jbig2/JBig2_SymbolDict.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a PDF document containing crafted data with JBIG2 compression. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6779 | None | None | PDFium, as used in Google Chrome before 47.0.2526.73, does not properly restrict use of chrome: URLs, which allows remote attackers to bypass intended scheme restrictions via a crafted PDF document, as demonstrated by a document with a link to a chrome://settings URL.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6780 | None | None | Use-after-free vulnerability in the Infobars implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site, related to browser/ui/views/website_settings/website_settings_popup_view.cc.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6781 | None | None | Integer overflow in the FontData::Bound function in data/font_data.cc in Google sfntly, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted offset or length value within font data in an SFNT container.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6782 | None | None | The Document::open function in WebKit/Source/core/dom/Document.cpp in Google Chrome before 47.0.2526.73 does not ensure that page-dismissal event handling is compatible with modal-dialog blocking, which makes it easier for remote attackers to spoof Omnibox content via a crafted web site.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6783 | None | None | The FindStartOffsetOfFileInZipFile function in crazy_linker_zip.cpp in crazy_linker (aka Crazy Linker) in Android 5.x and 6.x, as used in Google Chrome before 47.0.2526.73, improperly searches for an EOCD record, which allows attackers to bypass a signature-validation requirement via a crafted ZIP archive.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6784 | None | None | The page serializer in Google Chrome before 47.0.2526.73 mishandles Mark of the Web (MOTW) comments for URLs containing a "--" sequence, which might allow remote attackers to inject HTML via a crafted URL, as demonstrated by an initial http://example.com?-- substring.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6785 | None | None | The CSPSource::hostMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts an x.y hostname as a match for a *.x.y pattern, which might allow remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging a policy that was intended to be specific to subdomains.                        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6786 | None | None | The CSPSourceList::matches function in WebKit/Source/core/frame/csp/CSPSourceList.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts a blob:, data:, or filesystem: URL as a match for a * pattern, which allows remote attackers to bypass intended scheme restrictions in opportunistic circumstances by leveraging a policy that relies on this pattern.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6787 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.73 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-8478 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.73, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-8479 | None | None | Use-after-free vulnerability in the AudioOutputDevice::OnDeviceAuthorized function in media/audio/audio_output_device.cc in Google Chrome before 47.0.2526.73 allows attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering access to an unauthorized audio output device.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-8480 | None | None | The VideoFramePool::PoolImpl::CreateFrame function in media/base/video_frame_pool.cc in Google Chrome before 47.0.2526.73 does not initialize memory for a video-frame data structure, which might allow remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact by leveraging improper interaction with the vp3_h_loop_filter_c function in libavcodec/vp3dsp.c in FFmpeg. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6788 | None | None | The ObjectBackedNativeHandler class in extensions/renderer/object_backed_native_handler.c in the extensions subsystem in Google Chrome before 47.0.2526.80 improperly implements handler functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6789 | None | None | Race condition in the MutationObserver implementation in Blink, as used in Google Chrome before 47.0.2526.80, allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact by leveraging unanticipated object deletion.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6790 | None | None | The WebPageSerializerImpl::openTagToString function in WebKit/Source/web/WebPageSerializerImpl.cpp in the page serializer in Google Chrome before 47.0.2526.80 does not properly use HTML entities, which might allow remote attackers to inject arbitrary web script or HTML via a crafted document, as demonstrated by a double-quote character inside a single-quoted string. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6791 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.80 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-8548 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.80, allow attackers to cause a denial of service or possibly have other impact via unknown vectors, a different issue than CVE-2015-8478.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-6792 | None | None | The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-8664 | None | None | Integer overflow in the WebCursor::Deserialize function in content/common/cursors/webcursor.cc in Google Chrome before 47.0.2526.106 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an RGBA pixel array with crafted dimensions, a different vulnerability than CVE-2015-6792.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1612 | None | None | The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1613 | None | None | Multiple use-after-free vulnerabilities in the formfiller implementation in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to improper tracking of the destruction of (1) IPWL_FocusHandler and (2) IPWL_Provider objects.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1614 | None | None | The UnacceleratedImageBufferSurface class in WebKit/Source/platform/graphics/UnacceleratedImageBufferSurface.cpp in Blink, as used in Google Chrome before 48.0.2564.82, mishandles the initialization mode, which allows remote attackers to obtain sensitive information from process memory via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1615 | None | None | The Omnibox implementation in Google Chrome before 48.0.2564.82 allows remote attackers to spoof a document's origin via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1616 | None | None | The CustomButton::AcceleratorPressed function in ui/views/controls/button/custom_button.cc in Google Chrome before 48.0.2564.82 allows remote attackers to spoof URLs via vectors involving an unfocused custom button.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1617 | None | None | The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 48.0.2564.82, does not apply http policies to https URLs and does not apply ws policies to wss URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1618 | None | None | Blink, as used in Google Chrome before 48.0.2564.82, does not ensure that a proper cryptographicallyRandomValues random number generator is used, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1619 | None | None | Multiple integer overflows in the (1) sycc422_to_rgb and (2) sycc444_to_rgb functions in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted PDF document.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1620 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-2051 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.8.271.17, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-2052 | None | None | Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via crafted data, as demonstrated by a buffer over-read resulting from an inverted length check in hb-ot-font.cc, a different issue than CVE-2015-8947.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1622 | None | None | The Extensions subsystem in Google Chrome before 48.0.2564.109 does not prevent use of the Object.defineProperty method to override intended extension behavior, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1623 | None | None | The DOM implementation in Google Chrome before 48.0.2564.109 does not properly restrict frame-attach operations from occurring during or after frame-detach operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related to FrameLoader.cpp, HTMLFrameOwnerElement.h, LocalFrame.cpp, and WebLocalFrameImpl.cpp. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1624 | None | None | Integer underflow in the ProcessCommandsInternal function in dec/decode.c in Brotli, as used in Google Chrome before 48.0.2564.109, allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted data with brotli compression.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1625 | None | None | The Chrome Instant feature in Google Chrome before 48.0.2564.109 does not ensure that a New Tab Page (NTP) navigation target is on the most-visited or suggestions list, which allows remote attackers to bypass intended restrictions via unspecified vectors, related to instant_service.cc and search_tab_helper.cc.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1626 | None | None | The opj_pi_update_decode_poc function in pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, miscalculates a certain layer index value, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1627 | None | None | The Developer Tools (aka DevTools) subsystem in Google Chrome before 48.0.2564.109 does not validate URL schemes and ensure that the remoteBase parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL, related to browser/devtools/devtools_ui_bindings.cc and WebKit/Source/devtools/front_end/Runtime.js. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1628 | None | None | pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, does not validate a certain precision value, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via a crafted JPEG 2000 image in a PDF document, related to the opj_pi_next_rpcl, opj_pi_next_pcrl, and opj_pi_next_cpcl functions.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1629 | None | None | Google Chrome before 48.0.2564.116 allows remote attackers to bypass the Blink Same Origin Policy and a sandbox protection mechanism via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1630 | None | None | The ContainerNode::parserRemoveChild function in WebKit/Source/core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 49.0.2623.75, mishandles widget updates, which makes it easier for remote attackers to bypass the Same Origin Policy via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1631 | None | None | The PPB_Flash_MessageLoop_Impl::InternalRun function in content/renderer/pepper/ppb_flash_message_loop_impl.cc in the Pepper plugin in Google Chrome before 49.0.2623.75 mishandles nested message loops, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1632 | None | None | The Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly maintain own properties, which allows remote attackers to bypass intended access restrictions via crafted JavaScript code that triggers an incorrect cast, related to extensions/renderer/v8_helpers.h and gin/converter.h.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1633 | None | None | Use-after-free vulnerability in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1634 | None | None | Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1635 | None | None | extensions/renderer/render_frame_observer_natives.cc in Google Chrome before 49.0.2623.75 does not properly consider object lifetimes and re-entrancy issues during OnDocumentElementCreated handling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1636 | None | None | The PendingScript::notifyFinished function in WebKit/Source/core/dom/PendingScript.cpp in Google Chrome before 49.0.2623.75 relies on memory-cache information about integrity-check occurrences instead of integrity-check successes, which allows remote attackers to bypass the Subresource Integrity (aka SRI) protection mechanism by triggering two loads of the same resource.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1637 | None | None | The SkATan2_255 function in effects/gradients/SkSweepGradient.cpp in Skia, as used in Google Chrome before 49.0.2623.75, mishandles arctangent calculations, which allows remote attackers to obtain sensitive information via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1638 | None | None | extensions/renderer/resources/platform_app.js in the Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly restrict use of Web APIs, which allows remote attackers to bypass intended access restrictions via a crafted platform app.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1639 | None | None | Use-after-free vulnerability in browser/extensions/api/webrtc_audio_private/webrtc_audio_private_api.cc in the WebRTC Audio Private API implementation in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect reliance on the resource context pointer.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1640 | None | None | The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 does not block installations upon deletion of an installation frame, which makes it easier for remote attackers to trick a user into believing that an installation request originated from the user's next navigation target via a crafted web site.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1641 | None | None | Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.c c in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1642 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 49.0.2623.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-2843 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.9.385.26, as used in Google Chrome before 49.0.2623.75, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-2844 | None | None | WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code.                         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-2845 | None | None | The Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 49.0.2623.75, does not ignore a URL's path component in the case of a ServiceWorker fetch, which allows remote attackers to obtain sensitive information about visited web pages by reading CSP violation reports, related to FrameFetchContext.cpp and ResourceFetcher.cpp. |

|               |                    |               |                  |            |  |
|---------------|--------------------|---------------|------------------|------------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1643 | None             | None       | The ImageInputType::ensurePrimaryContent function in WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion." |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1644 | None             | None       | WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict layout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1645 | HIGH             | 8.8        | Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1646 | ['HIGH', 'HIGH'] | [8.8, 8.8] | The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1647 | None             | None       | Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1648 | None             | None       | Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1649 | None | None | The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome before 49.0.2623.108, does not properly handle a certain data-type mismatch, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted shader stages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1650 | None | None | The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-3679 | None | None | Multiple unspecified vulnerabilities in Google V8 before 4.9.385.33, as used in Google Chrome before 49.0.2623.108, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1651 | None | None | fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 50.0.2661.75, does not properly implement the sycc420_to_rgb and sycc422_to_rgb functions, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted JPEG 2000 data in a PDF document.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1652 | None | None | Cross-site scripting (XSS) vulnerability in the ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the Extensions subsystem in Google Chrome before 50.0.2661.75 allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1653 | None | None | The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75, mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1654 | None | None | The media subsystem in Google Chrome before 50.0.2661.75 does not initialize an unspecified data structure, which allows remote attackers to cause a denial of service (invalid read operation) via unknown vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1655 | None | None | Google Chrome before 50.0.2661.75 does not properly consider that frame removal may occur during callback execution, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1656 | None | None | The download implementation in Google Chrome before 50.0.2661.75 on Android allows remote attackers to bypass intended pathname restrictions via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1657 | None | None | The WebContentsImpl::FocusLocationBarByDefault function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 50.0.2661.75 mishandles focus for certain about:blank pages, which allows remote attackers to spoof the address bar via a crafted URL.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1658 | None | None | The Extensions subsystem in Google Chrome before 50.0.2661.75 incorrectly relies on GetOrigin method calls for origin comparisons, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1659 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1660 | None | None | Blink, as used in Google Chrome before 50.0.2661.94, mishandles assertions in the WTF::BitArray and WTF::double_conversion::Vector classes, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1661 | None | None | Blink, as used in Google Chrome before 50.0.2661.94, does not ensure that frames satisfy a check for the same renderer process in addition to a Same Origin Policy check, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted web site, related to BindingSecurity.cpp and DOMWindow.cpp. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1662 | None | None | extensions/renderer/gc_callback.cc in Google Chrome before 50.0.2661.94 does not prevent fallback execution once the Garbage Collection callback has started, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1663 | None | None | The SerializedScriptValue::transferArrayBuffers function in WebKit/Source/bindings/core/v8/SerializedScriptValue.cpp in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.94, mishandles certain array-buffer data structures, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1664 | None | None | The HistoryController::UpdateForCommit function in content/renderer/history_controller.cc in Google Chrome before 50.0.2661.94 mishandles the interaction between subframe forward navigations and other forward navigations, which allows remote attackers to spoof the address bar via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1665 | None | None | The JSGenericLowering class in compiler/js-generic-lowering.cc in Google V8, as used in Google Chrome before 50.0.2661.94, mishandles comparison operators, which allows remote attackers to obtain sensitive information via crafted JavaScript code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1666 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1667 | None | None | The TreeScope::adoptIfNeeded function in WebKit/Source/core/dom/TreeScope.cpp in the DOM implementation in Blink, as used in Google Chrome before 50.0.2661.102, does not prevent script execution during node-adoption operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1668 | None | None | The forEachForBinding function in WebKit/Source/bindings/core/v8/Iterable.h in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.102, uses an improper creation context, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1669 | HIGH | 8.8  | The Zone::New function in zone.cc in Google V8 before 5.0.71.47, as used in Google Chrome before 50.0.2661.102, does not properly determine when to expand certain memory allocations, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1670 | None | None | Race condition in the ResourceDispatcherHostImpl::BeginRequest function in content/browser/loader/resource_dispatcher_host_impl.cc in Google Chrome before 50.0.2661.102 allows remote attackers to make arbitrary HTTP requests by leveraging access to a renderer process and reusing a request ID.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1671 | None | None | Google Chrome before 50.0.2661.102 on Android mishandles / (slash) and \ (backslash) characters, which allows attackers to conduct directory traversal attacks via a file: URL, related to net/base/escape.cc and net/base/filename_util.cc.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1672 | None | None | The ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the extension bindings in Google Chrome before 51.0.2704.63 mishandles properties, which allows remote attackers to conduct bindings-interception attacks and bypass the Same Origin Policy via unspecified vectors. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1673 | None | None | Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1674 | None | None | The extensions subsystem in Google Chrome before 51.0.2704.63 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1675 | None | None | Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy by leveraging the mishandling of Document reattachment during destruction, related to FrameLoader.cpp and LocalFrame.cpp.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1676 | None | None | extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.63 does not properly use prototypes, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1677 | None | None | uri.js in Google V8 before 5.1.281.26, as used in Google Chrome before 51.0.2704.63, uses an incorrect array type, which allows remote attackers to obtain sensitive information by calling the decodeURI function and leveraging "type confusion."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1678 | None | None | objects.cc in Google V8 before 5.0.71.32, as used in Google Chrome before 51.0.2704.63, does not properly restrict lazy deoptimization, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.       |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1679 | None | None | The ToV8Value function in content/child/v8_value_converter_impl.cc in the V8 bindings in Google Chrome before 51.0.2704.63 does not properly restrict use of getters and setters, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1680 | None | None | Use-after-free vulnerability in ports/SkFontHost_FreeType.cpp in Skia, as used in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1681 | None | None | Heap-based buffer overflow in the opj_j2k_read_SPCod_SPCoc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1682 | None | None | The ServiceWorkerContainer::registerServiceWorker Impl function in WebKit/Source/modules/serviceworkers/ServiceWorkerContainer.cpp in Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a ServiceWorker registration.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1683 | None | None | numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which allows remote attackers to cause a denial of service (out-of-bounds heap memory access) or possibly have unspecified other impact via a crafted document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1684 | None | None | numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles the i format token for xsl:number data, which allows remote attackers to cause a denial of service (integer overflow or resource consumption) or possibly have unspecified other impact via a crafted document.                         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1685 | None | None | core/fxge/ge/fx_ge_text.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, miscalculates certain index values, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1686 | None | None | The CPDF_DIBSource::CreateDecoder function in core/fpdfapi/fpdf_render/fpdf_render_loadimage.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, mishandles decoder-initialization failure, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1687 | None | None | The renderer implementation in Google Chrome before 51.0.2704.63 does not properly restrict public exposure of classes, which allows remote attackers to obtain sensitive information via vectors related to extensions.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1688 | None | None | The regexp (aka regular expression) implementation in Google V8 before 5.0.71.40, as used in Google Chrome before 51.0.2704.63, mishandles external string sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted JavaScript code.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1689 | None | None | Heap-based buffer overflow in content/renderer/media/canvas_capture_handler.cc in Google Chrome before 51.0.2704.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1690 | None | None | The Autofill implementation in Google Chrome before 51.0.2704.63 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1701. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1691 | None | None | Skia, as used in Google Chrome before 51.0.2704.63, mishandles coincidence runs, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted curves, related to SkOpCoincidence.cpp and SkPathOpsCommon.cpp.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1692 | None | None | WebKit/Source/core/css/StyleSheetContents.cpp in Blink, as used in Google Chrome before 51.0.2704.63, permits cross-origin loading of CSS stylesheets by a ServiceWorker even when the stylesheet download has an incorrect MIME type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.                                     |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1693 | None | None | browser/safe_browsing/srt_field_trial_win.cc in Google Chrome before 51.0.2704.63 does not use the HTTPS service on dl.google.com to obtain the Software Removal Tool, which allows remote attackers to spoof the chrome_cleanup_tool.exe (aka CCT) file via a man-in-the-middle attack on an HTTP session.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1694 | None | None | browser/browsing_data/browsing_data_remover.cc in Google Chrome before 51.0.2704.63 deletes HPKP pins during cache clearing, which makes it easier for remote attackers to spoof web sites via a valid certificate from an arbitrary recognized Certification Authority.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1695 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.63 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1696 | None | None | The extensions subsystem in Google Chrome before 51.0.2704.79 does not properly restrict bindings access, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1697 | None | None | The FrameLoader::startLoad function in WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 51.0.2704.79, does not prevent frame navigations during DocumentLoader detach operations, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1698 | None | None | The createCustomType function in extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.79 does not validate module types, which might allow attackers to load arbitrary modules or obtain sensitive information by leveraging a poisoned definition.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1699 | None | None | WebKit/Source/devtools/front_end/devtools.js in the Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 51.0.2704.79, does not ensure that the remoteFrontendUrl parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1700 | None | None | extensions/renderer/runtime_custom_bindings.cc in Google Chrome before 51.0.2704.79 does not consider side effects during creation of an array of extension views, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to extensions.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1701 | None | None | The Autofill implementation in Google Chrome before 51.0.2704.79 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1690.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1702 | None | None | The SkRegion::readFromMemory function in core/SkRegion.cpp in Skia, as used in Google Chrome before 51.0.2704.79, does not validate the interval count, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted serialized data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1703 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.79 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1704 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.103 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1705 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1706 | None | None | The PPAPI implementation in Google Chrome before 52.0.2743.82 does not validate the origin of IPC messages to the plugin broker process that should have come from the browser process, which allows remote attackers to bypass a sandbox protection mechanism via an unexpected message type, related to broker_process_dispatcher.cc, ppapi_plugin_process_host.cc, ppapi_thread.cc, and render_frame_message_filter.cc. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1707 | None | None | ios/web/web_state/ui/crw_web_controller.mm in Google Chrome before 52.0.2743.82 on iOS does not ensure that an invalid URL is replaced with the about:blank URL, which allows remote attackers to spoof the URL display via a crafted web site.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1708 | None | None | The Chrome Web Store inline-installation implementation in the Extensions subsystem in Google Chrome before 52.0.2743.82 does not properly consider object lifetimes during progress observation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1709 | None | None | Heap-based buffer overflow in the ByteArray::GetMethod in data/byte_array.cc in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SFNT font.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1710 | None | None | The ChromeClientImpl::createWindow method in WebKit/Source/web/ChromeClientImpl.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not prevent window creation by a deferred frame, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-1711 | None | None | WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not disable frame navigation during a detach operation on a DocumentLoader object, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5127 | None | None | Use-after-free vulnerability in WebKit/Source/core/editing/VisibleUnits.cpp in Blink, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code involving an @import at-rule in a Cascading Style Sheets (CSS) token sequence in conjunction with a rel=import attribute of a LINK element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5128 | None | None | objects.cc in Google V8 before 5.2.361.27, as used in Google Chrome before 52.0.2743.82, does not prevent API interceptors from modifying a store target without setting a property, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5129 | None | None | Google V8 before 5.2.361.32, as used in Google Chrome before 52.0.2743.82, does not properly process left-trimmed objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5130 | None | None | content/renderer/history_controller.cc in Google Chrome before 52.0.2743.82 does not properly restrict multiple uses of a JavaScript forward method, which allows remote attackers to spoof the URL display via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5131 | None | None | Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to-function.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5132 | None | None | The Service Workers subsystem in Google Chrome before 52.0.2743.82 does not properly implement the Secure Contexts specification during decisions about whether to control a subframe, which allows remote attackers to bypass the Same Origin Policy via an https IFRAME element inside an http IFRAME element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5133 | None | None | Google Chrome before 52.0.2743.82 mishandles origin information during proxy authentication, which allows man-in-the-middle attackers to spoof a proxy-authentication login prompt or trigger incorrect credential storage by modifying the client-server data stream.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5134 | None | None | net/proxy/proxy_service.cc in the Proxy Auto-Config (PAC) feature in Google Chrome before 52.0.2743.82 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, a related issue to CVE-2016-3763.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5135 | None | None | WebKit/Source/core/html/parser/HTMLPreloadScanner.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not consider referrer-policy information inside an HTML document during a preload request, which allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a crafted web site, as demonstrated by a "Content-Security-Policy: referrer origin-when-cross-origin" header that overrides a "<META name='referrer' content='no-referrer'>" element. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5136 | None | None | Use-after-free vulnerability in extensions/renderer/user_script_injector.cc in the Extensions subsystem in Google Chrome before 52.0.2743.82 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to script deletion.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5137 | None | None | The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 52.0.2743.82, does not apply http :80 policies to https :443 URLs and does not apply ws :80 policies to wss :443 URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report. NOTE: this vulnerability is associated with a specification change after CVE-2016-1617 resolution. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5138 | None | None | Integer overflow in the kbasep_vinstr_attach_client function in midgard/mali_kbase_vinstr.c in Google Chrome before 52.0.2743.85 allows remote attackers to cause a denial of service (heap-based buffer overflow and use-after-free) by leveraging an unrestricted multiplication.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5139 | None | None | Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5140 | None | None | Heap-based buffer overflow in the opj_j2k_read_SQcd_SQcc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JPEG 2000 data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5141 | None | None | Blink, as used in Google Chrome before 52.0.2743.116, allows remote attackers to spoof the address bar via vectors involving a provisional URL for an initially empty document, related to FrameLoader.cpp and ScopedPageLoadDeferrer.cpp.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5142 | None | None | The Web Cryptography API (aka WebCrypto) implementation in Blink, as used in Google Chrome before 52.0.2743.116, does not properly copy data buffers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code, related to NormalizeAlgorithm.cpp and SubtleCrypto.cpp.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5143 | None | None | The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5144.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5144 | None | None | The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5143.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5145 | None | None | Blink, as used in Google Chrome before 52.0.2743.116, does not ensure that a taint property is preserved after a structure-clone operation on an ImageBitmap object derived from a cross-origin image, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5146 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5147 | None | None | Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles deferred page loads, which allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5148 | None | None | Cross-site scripting (XSS) vulnerability in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML via vectors related to widget updates, aka "Universal XSS (UXSS)."  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5149 | None | None | The extensions subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux relies on an IFRAME source URL to identify an associated extension, which allows remote attackers to conduct extension-bindings injection attacks by leveraging script access to a resource that initially has the about:blank URL. |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5150 | None | None | WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, has an Indexed Database (aka IndexedDB) API implementation that does not properly restrict key-path evaluation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code that leverages certain side effects. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5151 | None | None | PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux mishandles timers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/javascript/JS_Object.cpp and fpdfsdk/javascript/app.cpp.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5152 | None | None | Integer overflow in the opj_tcd_get_decoded_tile_size function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5153 | None | None | The Web Animations implementation in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, improperly relies on list iteration, which allows remote attackers to cause a denial of service (use-after-destruction) or possibly have unspecified other impact via a crafted web site.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5154 | None | None | Multiple heap-based buffer overflows in PDFium, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JBig2 image.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5155 | None | None | Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly validate access to the initial document, which allows remote attackers to spoof the address bar via a crafted web site.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5156 | None | None | extensions/renderer/event_bindings.cc in the event bindings in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux attempts to process filtered events after failure to add an event matcher, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5157 | None | None | Heap-based buffer overflow in the opj_dwt_interleave_v function in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to execute arbitrary code via crafted coordinate values in JPEG 2000 data.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5158 | None | None | Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5159 | None | None | Multiple integer overflows in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during opj_aligned_malloc calls in dwt.c and t1.c.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5160 | None | None | The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5162. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5161 | None | None | The EditingStyle::mergeStyle function in WebKit/Source/core/editing/EditingStyle.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles custom properties, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that leverages "type confusion" in the StylePropertySerializer class.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5162 | None | None | The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5160. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5163 | None | None | The bidirectional-text implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not ensure left-to-right (LTR) rendering of URLs, which allows remote attackers to spoof the address bar via crafted right-to-left (RTL) Unicode text, related to omnibox/SuggestionView.java and omnibox/UrlBar.java in Chrome for Android.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5164 | None | None | Cross-site scripting (XSS) vulnerability in WebKit/Source/platform/v8_inspector/V8Debugger.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML into the Developer Tools (aka DevTools) subsystem via a crafted web site, aka "Universal XSS (UXSS)."   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5165 | None | None | Cross-site scripting (XSS) vulnerability in the Developer Tools (aka DevTools) subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allows remote attackers to inject arbitrary web script or HTML via the settings parameter in a chrome-devtools-frontend.appspot.com URL's query string.   |

|               |                    |               |        |      |  |
|---------------|--------------------|---------------|--------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5166 | None   | None | The download implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly restrict saving a file:// URL that is referenced by an http:// URL, which makes it easier for user-assisted remote attackers to discover NetNTLM hashes and conduct SMB relay attacks via a crafted web page that is accessed with the "Save page as" menu choice. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5167 | None   | None | Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-7395 | None   | None | SkPath.cpp in Skia, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, does not properly validate the return values of ChopMonoAtY calls, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via crafted graphics data.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5169 | None   | None | Format string vulnerability in Google Chrome OS before 53.0.2785.103 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5170 | None   | None | WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not properly consider getter side effects during array key conversion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Indexed Database (aka IndexedDB) API calls.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5171 | None   | None | WebKit/Source/bindings/templates/interface.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not prevent certain constructor calls, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5172 | MEDIUM | 6.5  | The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5173 | None | None | The extensions subsystem in Google Chrome before 53.0.2785.113 does not properly restrict access to Object.prototype, which allows remote attackers to load unintended resources, and consequently trigger unintended JavaScript function calls and bypass the Same Origin Policy via an indirect interception attack.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5174 | None | None | browser/ui/cocoa/browser_window_controller_private.mm in Google Chrome before 53.0.2785.113 does not process fullscreen toggle requests during a fullscreen transition, which allows remote attackers to cause a denial of service (unsuppressed popup) via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5175 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.113 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-7549 | None | None | Google Chrome before 53.0.2785.113 does not ensure that the recipient of a certain IPC message is a valid RenderFrame or RenderWidget, which allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) or possibly have unspecified other impact by leveraging access to a renderer process, related to render_frame_host_impl.cc and render_widget_host_impl.cc, as demonstrated by a Password Manager message. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5176 | None | None | Google Chrome before 53.0.2785.113 allows remote attackers to bypass the SafeBrowsing protection mechanism via unspecified vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5181 | None | None | Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5182 | None | None | Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5183 | None | None | A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5184 | None | None | PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFiller::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5185 | None | None | Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5186 | None | None | Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5187 | None | None | Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5188 | None | None | Multiple issues in Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux allow a remote attacker to spoof various parts of browser UI via crafted HTML pages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5189 | None | None | Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5190 | None | None | Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5191 | None | None | Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation of supplied data, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages, as demonstrated by an interpretation conflict between userinfo and scheme in an http://javascript:payload@example.com URL. |

|               |                    |               |                  |            |   |
|---------------|--------------------|---------------|------------------|------------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5192 | None             | None       | Blink in Google Chrome prior to 54.0.2840.59 for Windows missed a CORS check on redirect in TextTrackLoader, which allowed a remote attacker to bypass cross-origin restrictions via crafted HTML pages.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5193 | None             | None       | Google Chrome prior to 54.0 for iOS had insufficient validation of URLs for windows open by DOM, which allowed a remote attacker to bypass restrictions on navigation to certain URL schemes via crafted HTML pages.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5196 | None             | None       | The content renderer client in Google Chrome prior to 54.0.2840.85 for Android insufficiently enforced the Same Origin Policy amongst downloaded files, which allowed a remote attacker to access any downloaded file and interact with sites, including those the user was logged into, via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5197 | None             | None       | The content view client in Google Chrome prior to 54.0.2840.85 for Android insufficiently validated intent URLs, which allowed a remote attacker who had compromised the renderer process to start arbitrary activity on the system via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5198 | ['HIGH', 'HIGH'] | [8.8, 8.8] | V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5199 | None             | None       | An off by one error resulting in an allocation of zero size in FFmpeg in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted video file.          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5200 | None             | None       | V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5201 | None             | None       | A leak of privateClass in the extensions API in Google Chrome prior to 54.0.2840.100 for Linux, and 54.0.2840.99 for Windows, and 54.0.2840.98 for Mac allowed a remote attacker to access privileged JavaScript code via a crafted HTML page.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5203 | None | None | A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5204 | None | None | Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5205 | None | None | Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac, incorrectly handles deferred page loads, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5206 | None | None | The PDF plugin in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly followed redirects, which allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5207 | None | None | In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5208 | None | None | Blink in Google Chrome prior to 55.0.2883.75 for Linux and Windows, and 55.0.2883.84 for Android allowed possible corruption of the DOM tree during synchronous event handling, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5209 | None | None | Bad casting in bitmap manipulation in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5210 | None | None | Heap buffer overflow during TIFF image parsing in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5211 | None | None | A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5212 | None | None | Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android insufficiently sanitized DevTools URLs, which allowed a remote attacker to read local files via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5213 | None | None | A use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5214 | None | None | Google Chrome prior to 55.0.2883.75 for Windows mishandled downloaded files, which allowed a remote attacker to prevent the downloaded file from receiving the Mark of the Web via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5215 | None | None | A use after free in webaudio in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5216 | None | None | A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5217 | None | None | The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly permitted access to privileged plugins, which allowed a remote attacker to bypass site isolation via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5218 | None | None | The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to temporarily spoof the contents of the Omnibox (URL bar) via a crafted HTML page containing PDF data. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5219 | None | None | A heap use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5220 | None | None | PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to read local files via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5221 | None | None | Type confusion in libGLESv2 in ANGLE in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android possibly allowed a remote attacker to bypass buffer validation via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5222 | None | None | Incorrect handling of invalid URLs in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5223 | None | None | Integer overflow in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption or DoS via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5224 | None | None | A timing attack on denormalized floating point arithmetic in SVG filters in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5225 | None | None | Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled form actions, which allowed a remote attacker to bypass Content Security Policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5226 | None | None | Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac executed javascript: URLs entered in the URL bar in the context of the current tab, which allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-9650 | None | None | Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled iframes, which allowed a remote attacker to bypass a no-referrer policy via a crafted HTML page.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-3823 | None | None | An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programming interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link wit... |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5006 | None | None | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5007 | None | None | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5008 | None | None | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5009 | None | None | WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5010 | None | None | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5011 | None | None | Google Chrome prior to 56.0.2924.76 for Windows insufficiently sanitized DevTools URLs, which allowed a remote attacker who convinced a user to install a malicious extension to read filesystem contents via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5012 | None | None | A heap buffer overflow in V8 in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5013 | None | None | Google Chrome prior to 56.0.2924.76 for Linux incorrectly handled new tab page navigations in non-selected tabs, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5014 | None | None | Heap buffer overflow during image processing in Skia in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5015 | None | None | Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5016 | None | None | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5017 | None | None | Interactions with the OS in Google Chrome prior to 56.0.2924.76 for Mac insufficiently cleared video memory, which allowed a remote attacker to possibly extract image fragments on systems with GeForce 8600M graphics chips via a crafted HTML page.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5018 | None | None | Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, had an insufficiently strict content security policy on the Chrome app launcher page, which allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5019 | None | None | A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5020 | None | None | Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations, which allowed a remote attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5021 | None | None | A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5022 | None | None | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.                                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5023 | None | None | Type confusion in Histogram in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit a near null dereference via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5024 | None | None | FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5025 | None | None | FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.  |

|               |                    |               |                  |            |  |
|---------------|--------------------|---------------|------------------|------------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5026 | None             | None       | Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to prevent alerts from being displayed by swapped out frames, which allowed a remote attacker to show alerts on a page they don't control via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5027 | None             | None       | Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6647 | None             | None       | A use-after-free in AnimationController::endAnimationUpdate in Google Chrome.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2013-6662 | None             | None       | Google Chrome caches TLS sessions before certificate validation occurs.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5168 | None             | None       | Skia, as used in Google Chrome before 50.0.2661.94, allows remote attackers to bypass the Same Origin Policy and obtain sensitive information.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-9654 | None             | None       | The Regular Expressions package in International Components for Unicode (ICU) for C/C++ before 2014-12-03, as used in Google Chrome before 40.0.2214.91, calculates certain values without ensuring that they can be represented in a 24-bit field, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted string, a related issue to CVE-2014-7923. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5029 | HIGH             | 8.8        | The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5030 | ['HIGH', 'HIGH'] | [8.8, 8.8] | Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5031 | None             | None       | A use after free in ANGLE in Google Chrome prior to 57.0.2987.98 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5032 | None             | None       | PDFium in Google Chrome prior to 57.0.2987.98 for Windows could be made to increment off the end of a buffer, which allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.   |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5033 | MEDIUM | 4.3  | Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android failed to correctly propagate CSP restrictions to local scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page, related to the unsafe-inline keyword. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5034 | None   | None | A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5035 | HIGH   | 8.1  | Google Chrome prior to 57.0.2987.98 for Windows and Mac had a race condition, which could cause Chrome to display incorrect certificate information for a site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5036 | HIGH   | 7.8  | A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to have an unspecified impact via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5037 | HIGH   | 7.8  | An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5038 | MEDIUM | 6.3  | Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5039 | HIGH   | 7.8  | A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5040 | MEDIUM | 4.3  | V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android was missing a neutering check, which allowed a remote attacker to read values in memory via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5041 | None   | None | Google Chrome prior to 57.0.2987.100 incorrectly handled back-forward navigation, which allowed a remote attacker to display incorrect information for a site via a crafted HTML page.  |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5042 | MEDIUM | 5.7  | Cast in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android sent cookies to sites discovered via SSDP, which allowed an attacker on the local network segment to initiate connections to arbitrary URLs and observe any plaintext cookies sent. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5043 | HIGH   | 8.8  | Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5044 | MEDIUM | 6.3  | Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5045 | MEDIUM | 6.1  | XSS Auditor in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed detection of a blocked iframe load, which allowed a remote attacker to brute force JavaScript variables via a crafted HTML page.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5046 | MEDIUM | 4.3  | V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android had insufficient policy enforcement, which allowed a remote attacker to spoof the location object via a crafted HTML page, related to Blink information disclosure.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5047 | None   | None | An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5048 | None   | None | An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5049 | None   | None | An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5050 | None   | None | An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.                                      |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5051 | None | None | An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5177 | None | None | Use-after-free vulnerability in V8 in Google Chrome before 53.0.2785.143 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via unknown vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5178 | None | None | Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.143 allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1207 | None | None | Double-free vulnerability in libavformat/mov.c in FFMPEG in Google Chrome 41.0.2251.0 allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted .m4a file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-0959 | None | None | Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233. |

|               |                    |               |          |      |  |
|---------------|--------------------|---------------|----------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-6753 | None     | None | A vulnerability in Cisco WebEx browser extensions for Google Chrome and Mozilla Firefox could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server, Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center), and Cisco WebEx Meetings when they are running on Microsoft Windows. The vulnerability is due to a design defect in the extension. An attacker who can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser. The following versions of the Cisco WebEx browser extensions are affected: Versions prior to 1.0.12 of the Cisco WebEx extension on Google Chrome, Versions prior to 1.0.12 of the Cis... |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-3880 | None     | None | Open redirect vulnerability in phpBB before 3.0.14 and 3.1.x before 3.1.4 allows remote attackers to redirect users of Google Chrome to arbitrary web sites and conduct phishing attacks via unspecified vectors.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1206 | None     | None | Heap-based buffer overflow in Google Chrome before M40 allows remote attackers to cause a denial of service (unpaged memory write and process crash) via a crafted MP4 file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1239 | MEDIUM   | 6.5  | Double free vulnerability in the j2k_read_ppm_v3 function in OpenJPEG before r2997, as used in PDFium in Google Chrome, allows remote attackers to cause a denial of service (process crash) via a crafted PDF.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5052 | HIGH     | 8.8  | An incorrect assumption about block structure in Blink in Google Chrome prior to 57.0.2987.133 for Mac, Windows, and Linux, and 57.0.2987.132 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page that triggers improper casting.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5053 | CRITICAL | 9.6  | An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to Array.prototype.indexOf.  |

|               |                    |               |        |      |  |
|---------------|--------------------|---------------|--------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5054 | HIGH   | 8.8  | An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to obtain heap memory contents via a crafted HTML page.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5055 | None   | None | A use after free in printing in Google Chrome prior to 57.0.2987.133 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5056 | HIGH   | 8.8  | A use after free in Blink in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5057 | HIGH   | 8.8  | Type confusion in PDFium in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5058 | None   | None | A use after free in PrintPreview in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5059 | HIGH   | 8.8  | Type confusion in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to potentially obtain code execution via a crafted HTML page.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5060 | MEDIUM | 6.5  | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5061 | MEDIUM | 5.3  | A race condition in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5062 | HIGH   | 8.8  | A use after free in Chrome Apps in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to potentially perform out of bounds memory access via a crafted Chrome extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5063 | HIGH   | 8.8  | A numeric overflow in Skia in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.                        |

|               |                    |               |                  |            |   |
|---------------|--------------------|---------------|------------------|------------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5064 | None             | None       | Incorrect handling of DOM changes in Blink in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5065 | MEDIUM           | 4.7        | Lack of an appropriate action on page navigation in Blink in Google Chrome prior to 58.0.3029.81 for Windows and Mac allowed a remote attacker to potentially confuse a user into making an incorrect security decision via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5066 | MEDIUM           | 6.5        | Insufficient consistency checks in signature handling in the networking stack in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to incorrectly accept a badly formed X.509 certificate via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5067 | MEDIUM           | 6.5        | An insufficient watchdog timer in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5068 | HIGH             | 7.5        | Incorrect handling of picture ID in WebRTC in Google Chrome prior to 58.0.3029.96 for Mac, Windows, and Linux allowed a remote attacker to trigger a race condition via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5069 | MEDIUM           | 6.1        | Incorrect MIME type of XSS-Protection reports in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to circumvent Cross-Origin Resource Sharing checks via a crafted HTML page.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5070 | ['HIGH', 'HIGH'] | [8.8, 8.8] | Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5071 | MEDIUM           | 6.3        | Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows and Mac, and 59.0.3071.92 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5072 | None             | None       | Inappropriate implementation in Omnibox in Google Chrome prior to 59.0.3071.92 for Android allowed a remote attacker to perform domain spoofing with RTL characters via a crafted URL page.   |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5073 | HIGH   | 8.8  | Use after free in print preview in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5074 | None   | None | A use after free in Chrome Apps in Google Chrome prior to 59.0.3071.86 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, related to Bluetooth.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5075 | MEDIUM | 4.3  | Inappropriate implementation in CSP reporting in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to obtain the value of url fragments via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5076 | MEDIUM | 6.5  | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5077 | HIGH   | 8.8  | Insufficient validation of untrusted input in Skia in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5078 | HIGH   | 8.8  | Insufficient validation of untrusted input in Blink's mailto: handling in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac allowed a remote attacker to perform command injection via a crafted HTML page, a similar issue to CVE-2004-0121. For example, characters such as * have an incorrect interaction with xdg-email in xdg-utils, and a space character can be used in front of a command-line argument. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5079 | MEDIUM | 4.3  | Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5080 | None   | None | A use after free in credit card autofill in Google Chrome prior to 59.0.3071.86 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5081 | LOW    | 3.3  | Lack of verification of an extension's locale folder in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed an attacker with local write access to modify extensions by modifying extension files.     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5082 | None   | None | Failure to take advantage of available mitigations in credit card autofill in Google Chrome prior to 59.0.3071.92 for Android allowed a local attacker to take screen shots of credit card information via a crafted HTML page.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5083 | MEDIUM | 4.3  | Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5084 | None   | None | Inappropriate implementation in image-burner in Google Chrome OS prior to 59.0.3071.92 allowed a local attacker to read local files via dbus-send commands to a BurnImage D-Bus endpoint.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5085 | None   | None | Inappropriate implementation in Bookmarks in Google Chrome prior to 59 for iOS allowed a remote attacker who convinced the user to perform certain operations to run JavaScript on chrome:// pages via a crafted bookmark.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5086 | MEDIUM | 6.5  | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Windows and Mac allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5087 | HIGH   | 8.8  | A use after free in Blink in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, aka an IndexedDB sandbox escape. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5088 | HIGH   | 8.8  | Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5089 | MEDIUM | 6.5  | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.104 for Mac allowed a remote attacker to perform domain spoofing via a crafted domain name.  |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5090 | None   | None | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.115 for Mac allowed a remote attacker to perform domain spoofing via a crafted domain name containing a U+0620 character, aka Apple rdar problem 32458012.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5091 | HIGH   | 8.8  | A use after free in IndexedDB in Google Chrome prior to 60.0.3112.78 for Linux, Android, Windows, and Mac allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5092 | None   | None | Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5093 | MEDIUM | 6.5  | Inappropriate implementation in modal dialog handling in Blink in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to prevent a full screen warning from being displayed via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5094 | MEDIUM | 6.5  | Type confusion in extensions JavaScript bindings in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted HTML page.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5095 | HIGH   | 8.8  | Stack overflow in PDFium in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit stack corruption via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5096 | None   | None | Insufficient policy enforcement during navigation between different schemes in Google Chrome prior to 60.0.3112.78 for Android allowed a remote attacker to perform cross origin content download via a crafted HTML page, related to intents.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5097 | None   | None | Insufficient validation of untrusted input in Skia in Google Chrome prior to 60.0.3112.78 for Linux allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5098 | HIGH   | 8.8  | A use after free in V8 in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5099 | None   | None | Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to potentially gain privilege elevation via a crafted HTML page.   |

|               |                    |               |        |     |  |
|---------------|--------------------|---------------|--------|-----|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5100 | HIGH   | 8.8 | A use after free in Apps in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5101 | MEDIUM | 6.5 | Inappropriate implementation in Omnibox in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5102 | MEDIUM | 4.3 | Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5103 | MEDIUM | 4.3 | Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.                        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5104 | MEDIUM | 6.5 | Inappropriate implementation in interstitials in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to spoof the contents of the omnibox via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5105 | MEDIUM | 6.5 | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5106 | MEDIUM | 6.5 | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5107 | MEDIUM | 5.3 | A timing attack in SVG rendering in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to extract pixel values from a cross-origin page being iframe'd via a crafted HTML page.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5108 | HIGH   | 8.8 | Type confusion in PDFium in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5109 | MEDIUM | 4.3 | Inappropriate implementation of unload handler handling in permission prompts in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page. |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5110 | MEDIUM | 6.5  | Inappropriate implementation of the web payments API on blob: and data: schemes in Web Payments in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5111 | HIGH   | 8.8  | A use after free in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5112 | None   | None | Heap buffer overflow in WebGL in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5113 | HIGH   | 8.8  | Math overflow in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5114 | HIGH   | 8.8  | Inappropriate use of partition alloc in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5115 | None   | None | Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5116 | HIGH   | 8.8  | Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5117 | None   | None | Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Linux and Windows allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5118 | MEDIUM | 4.3  | Blink in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, failed to correctly propagate CSP restrictions to javascript scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page. |

|               |                    |                |        |      |   |
|---------------|--------------------|----------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5119  | None   | None | Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5120  | MEDIUM | 6.5  | Inappropriate use of www mismatch redirects in browser navigation in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially downgrade HTTPS requests to HTTP via a crafted HTML page. In other words, Chrome could transmit cleartext even though the user had entered an https URL, because of a misdesigned workaround for cases where the domain name in a URL almost matches the domain name in an X.509 server certificate (but differs in the initial "www." substring). |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5121  | HIGH   | 8.8  | Inappropriate use of JIT optimisation in V8 in Google Chrome prior to 61.0.3163.100 for Linux, Windows, and Mac allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to the escape analysis phase.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5122  | None   | None | Inappropriate use of table size handling in V8 in Google Chrome prior to 61.0.3163.100 for Windows allowed a remote attacker to trigger out-of-bounds access via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2015-1290  | None   | None | The Google V8 engine, as used in Google Chrome before 44.0.2403.89 and QtWebEngineCore in Qt before 5.5.1, allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted web site.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15386 | None   | None | Incorrect implementation in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15387 | None   | None | Insufficient enforcement of Content Security Policy in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to open javascript: URL windows when they should not be allowed to via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15388 | None   | None | Iteration through non-finite points in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |

|               |                    |                |      |      |   |
|---------------|--------------------|----------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15389 | None | None | An insufficient watchdog timer in navigation in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15390 | None | None | Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15391 | None | None | Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to access Extension pages without authorisation via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15392 | None | None | Insufficient data validation in V8 in Google Chrome prior to 62.0.3202.62 allowed an attacker who can write to the Windows Registry to potentially exploit heap corruption via a crafted Windows Registry entry, related to PlatformIntegration.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15393 | None | None | Insufficient Policy Enforcement in Devtools remote debugging in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to obtain access to remote debugging functionality via a crafted HTML page, aka a Referer leak.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15394 | None | None | Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing in permission dialogs via IDN homographs in a crafted Chrome Extension.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15395 | None | None | A use after free in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an ImageCapture NULL pointer dereference.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15397 | None | None | Inappropriate implementation in ChromeVox in Google Chrome OS prior to 62.0.3202.74 allowed a remote attacker in a privileged network position to observe or tamper with certain cleartext HTTP requests by leveraging that position.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15400 | None | None | Insufficient restriction of IPP filters in CUPS in Google Chrome OS prior to 62.0.3202.74 allowed a remote attacker to execute a command with the same privileges as the cups daemon via a crafted PPD file, aka a printer zeroconfig CRLF issue. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5124  | None | None | Incorrect application of sandboxing in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted MHTML page.  |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5125  | None | None | Heap buffer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5126  | None | None | A use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5127  | None | None | Use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5128  | None | None | Heap buffer overflow in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, related to WebGL.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5129  | None | None | A use after free in WebAudio in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5130  | None | None | An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5131  | None | None | An integer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an out-of-bounds write.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5132  | None | None | Inappropriate implementation in V8 in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka incorrect WebAssembly stack manipulation.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5133  | None | None | Off-by-one read/write on the heap in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to corrupt memory and possibly leak information and potentially execute code via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-10584 | None | None | dalek-browser-chrome-canary provides Google Chrome bindings for DalekJS.<br>dalek-browser-chrome-canary downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server. |

|               |                    |                |      |      |   |
|---------------|--------------------|----------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-10604 | None | None | dalek-browser-chrome is Google Chrome bindings for DalekJS. dalek-browser-chrome downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-10624 | None | None | selenium-chromedriver is a simple utility for downloading the Selenium Webdriver for Google Chrome selenium-chromedriver downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-12716 | None | None | The API service on Google Home and Chromecast devices before mid-July 2018 does not prevent DNS rebinding attacks from reading the scan_results JSON data, which allows remote attackers to determine the physical location of most web browsers by leveraging the presence of one of these devices on its local network, extracting the scan_results bssid fields, and sending these fields in a geolocation/v1/geolocate Google Maps Geolocation API request. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15407 | None | None | Out-of-bounds Write in the QUIC networking stack in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to gain code execution via a malicious server.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15408 | None | None | Heap buffer overflow in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file that is mishandled by PDFium.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15409 | None | None | Heap buffer overflow in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15410 | None | None | Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15411 | None | None | Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15412 | None | None | Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15413 | None | None | Type confusion in WebAssembly in V8 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15415 | None | None | Incorrect serialization in IPC in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the value of a pointer via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15416 | None | None | Heap buffer overflow in Blob API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka a Blink out-of-bounds read.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15417 | None | None | Inappropriate implementation in Skia canvas composite operations in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15418 | None | None | Use of uninitialized memory in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15419 | None | None | Insufficient policy enforcement in Resource Timing API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to infer browsing history by triggering a leaked cross-origin URL via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15420 | None | None | Incorrect handling of back navigations in error pages in Navigation in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15422 | None | None | Integer overflow in international date handling in International Components for Unicode (ICU) for C/C++ before 60.1, as used in V8 in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15423 | None | None | Inappropriate implementation in BoringSSL SPAKE2 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the low-order bits of SHA512(password) by inspecting protocol traffic.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15424 | None | None | Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.  |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15425 | None | None | Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15426 | None | None | Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15427 | None | None | Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15430 | None | None | Insufficient data validation in Chromecast plugin in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15396 | None | None | A stack buffer overflow in NumberingSystem in International Components for Unicode (ICU) for C/C++ before 60.2, as used in V8 in Google Chrome prior to 62.0.3202.75 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15398 | None | None | A stack buffer overflow in the QUIC networking stack in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to gain code execution via a malicious server.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15399 | None | None | A use after free in V8 in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15406 | None | None | A stack buffer overflow in V8 in Google Chrome prior to 62.0.3202.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15429 | None | None | Inappropriate implementation in V8 WebAssembly JS bindings in Google Chrome prior to 63.0.3239.108 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6031  | None | None | Use after free in PDFium in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6032 | None | None | Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted HTML page.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6033 | None | None | Insufficient data validation in Downloads in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6034 | None | None | Insufficient data validation in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6035 | None | None | Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6036 | None | None | Insufficient data validation in V8 in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user data via a crafted HTML page.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6037 | None | None | Inappropriate implementation in autofill in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain autofill data with insufficient user gestures via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6038 | None | None | Heap buffer overflow in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6039 | None | None | Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6040 | None | None | Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially bypass content security policy via a crafted HTML page.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6041 | None | None | Incorrect security UI in navigation in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6042 | None | None | Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.                    |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6043 | None | None | Insufficient data validation in External Protocol Handler in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially execute arbitrary programs on user machine via a crafted HTML page.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6045 | None | None | Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6046 | None | None | Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6047 | None | None | Insufficient policy enforcement in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user redirect URL via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6048 | None | None | Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referrer information via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6049 | None | None | Incorrect security UI in permissions prompt in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the origin to which permission is granted via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6050 | None | None | Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6051 | None | None | XSS Auditor in Google Chrome prior to 64.0.3282.119, did not ensure the reporting URL was in the same origin as the page it was on, which allowed a remote attacker to obtain referrer details via a crafted HTML page.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6052 | None | None | Lack of support for a non standard no-referrer policy value in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain referrer details from a web page that had thought it had opted out of sending referrer data. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6053 | None | None | Inappropriate implementation in New Tab Page in Google Chrome prior to 64.0.3282.119 allowed a local attacker to view website thumbnail images after clearing browser data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6054 | None | None | Use after free in WebUI in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.  |

|               |                    |                |                  |            |  |
|---------------|--------------------|----------------|------------------|------------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6055  | None             | None       | Insufficient policy enforcement in Catalog Service in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted HTML page.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6119  | None             | None       | Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17462 | None             | None       | Incorrect refcounting in AppCache in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform a sandbox escape via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17463 | ['HIGH', 'HIGH'] | [8.8, 8.8] | Incorrect side effect annotation in V8 in Google Chrome prior to 70.0.3538.64 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17464 | None             | None       | Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17465 | None             | None       | Incorrect implementation of object trimming in V8 in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17466 | None             | None       | Incorrect texture handling in Angle in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17467 | None             | None       | Insufficiently quick clearing of stale rendered content in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17468 | None             | None       | Incorrect handling of timer information during navigation in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obtain cross origin URLs via a crafted HTML page.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17469 | None             | None       | Incorrect handling of PDF filter chains in PDFium in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17471 | None             | None       | Incorrect dialog placement in WebContents in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.   |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17472 | None | None | Incorrect handling of googlechrome:// URL scheme on iOS in Intents in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to escape the <iframe> sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17473 | None | None | Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17474 | None | None | Use after free in HTMLImportsController in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17475 | None | None | Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17476 | None | None | Incorrect dialog placement in Cast UI in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17477 | None | None | Incorrect dialog placement in Extensions in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of extension popups via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6057  | None | None | Lack of special casing of Android ashmem in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to bypass inter-process read only guarantees via a crafted HTML page.          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6060  | None | None | Use after free in WebAudio in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6061  | None | None | A race in the handling of SharedArrayBuffers in WebAssembly in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6062  | None | None | Heap overflow write in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6063  | None | None | Incorrect use of mojo::WrapSharedMemoryHandle in Mojo in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. |

|               |                    |               |                  |            |   |
|---------------|--------------------|---------------|------------------|------------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6064 | None             | None       | Type Confusion in the implementation of <code>__defineGetter__</code> in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6065 | ['HIGH', 'HIGH'] | [8.8, 8.8] | Integer overflow in computing the required allocation size when instantiating a new javascript object in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6066 | None             | None       | Lack of CORS checking by ResourceFetcher/ResourceLoader in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6067 | None             | None       | Incorrect IPC serialization in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6068 | None             | None       | Object lifecycle issue in Chrome Custom Tab in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6069 | None             | None       | Stack buffer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6070 | None             | None       | Lack of CSP enforcement on WebUI pages in Bink in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6071 | None             | None       | An integer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6072 | None             | None       | An integer overflow leading to use after free in PDFium in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6073 | None             | None       | A heap buffer overflow in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6074 | None             | None       | Failure to apply Mark-of-the-Web in Downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to bypass OS level controls via a crafted HTML page.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6075 | None | None | Incorrect handling of specified filenames in file downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page and user interaction.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6076 | None | None | Insufficient encoding of URL fragment identifiers in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform a DOM based XSS attack via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6077 | None | None | Displacement map filters being applied to cross-origin images in Blink SVG rendering in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6078 | None | None | Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6079 | None | None | Inappropriate sharing of TEXTURE_2D_ARRAY/TEXTURE_3D data between tabs in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6080 | None | None | Lack of access control checks in Instrumentation in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to obtain memory metadata from privileged processes .                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6081 | None | None | XSS vulnerabilities in Interstitials in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension or open Developer Console to inject arbitrary scripts or HTML via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6082 | None | None | Including port 22 in the list of allowed FTP ports in Networking in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially enumerate internal host services via a crafted HTML page.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6083 | None | None | Failure to disallow PWA installation from CSP sandboxed pages in AppManifest in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to access privileged APIs via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6085 | None | None | Re-entry of a destructor in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6086 | None | None | A double-eviction in the Incognito mode cache that lead to a user-after-free in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6087 | None | None | A use-after-free in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6088 | None | None | An iterator-invalidation bug in PDFium in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6089 | None | None | A lack of CORS checks, after a Service Worker redirected to a cross-origin PDF, in Service Worker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6090 | None | None | An integer overflow that lead to a heap buffer-overflow in Skia in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6092 | None | None | An integer overflow on 32-bit systems in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.                                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6094 | None | None | Inline metadata in GarbageCollection in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6095 | None | None | Inappropriate dismissal of file picker on keyboard events in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to read local files via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6098 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.                        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6099 | None | None | A lack of CORS checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6101 | None | None | A lack of host validation in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page, if the user is running a remote DevTools debugging server. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6102 | None | None | Missing confusable characters in Internationalization in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6103 | None | None | A stagnant permission prompt in Prompts in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass permission policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6104 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6105 | None | None | Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6107 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6108 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6115 | None | None | Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially bypass OS malware checks via a crafted HTML page.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6116 | None | None | A nullptr dereference in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.                                    |

|               |                    |                |                  |            |  |
|---------------|--------------------|----------------|------------------|------------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6152  | None             | None       | The implementation of the Page.downloadBehavior backend unconditionally marked downloaded files as safe, regardless of file type in Google Chrome prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page and user interaction. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17480 | ['HIGH', 'HIGH'] | [8.8, 8.8] | Execution of user supplied Javascript during array deserialization leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17481 | None             | None       | Incorrect object lifecycle handling in PDFium in Google Chrome prior to 71.0.3578.98 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18335 | None             | None       | Heap buffer overflow in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18336 | None             | None       | Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18337 | None             | None       | Incorrect handling of stylesheets leading to a use after free in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18338 | None             | None       | Incorrect, thread-unsafe use of SkImage in Canvas in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18339 | None             | None       | Incorrect object lifecycle in WebAudio in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18340 | None             | None       | Incorrect object lifecycle in MediaRecorder in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18341 | None             | None       | An integer overflow leading to a heap buffer overflow in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |

|               |                    |                |      |      |   |
|---------------|--------------------|----------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18342 | None | None | Execution of user supplied Javascript during object deserialization can update object length leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18343 | None | None | Incorrect handling of paths leading to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18344 | None | None | Inappropriate allowance of the setDownloadBehavior devtools protocol feature in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker with control of an installed extension to access files on the local file system via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18345 | None | None | Incorrect handling of blob URLs in Site Isolation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker who had compromised the renderer process to bypass site isolation protections via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18346 | None | None | Incorrect handling of alert box display in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to present confusing browser UI via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18347 | None | None | Incorrect handling of failed navigations with invalid URLs in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to trick a user into executing javascript in an arbitrary origin via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18348 | None | None | Incorrect handling of bidirectional domain names with RTL characters in Omnibox in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18349 | None | None | Remote frame navigations was incorrectly permitted to local resources in Blink in Google Chrome prior to 71.0.3578.80 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18350 | None | None | Incorrect handling of CSP enforcement during navigations in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass content security policy via a crafted HTML page.   |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18351 | None | None | Lack of proper validation of ancestor frames site when sending lax cookies in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass SameSite cookie policy via a crafted HTML page.                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18352 | None | None | Service works could inappropriately gain access to cross origin audio in Media in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass same origin policy for audio content via a crafted HTML page.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18353 | None | None | Failure to dismiss http auth dialogs on navigation in Network Authentication in Google Chrome on Android prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of an auto dialog via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18354 | None | None | Insufficient validate of external protocols in Shell Integration in Google Chrome on Windows prior to 71.0.3578.80 allowed a remote attacker to launch external programs via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18355 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18356 | None | None | An integer overflow in path handling lead to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18357 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18358 | None | None | Lack of special casing of localhost in WPAD files in Google Chrome prior to 71.0.3578.80 allowed an attacker on the local network segment to proxy resources on localhost via a crafted WPAD file.                                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-18359 | None | None | Incorrect handling of Reflect.construct in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-10403 | None | None | Insufficient data validation on image data in PDFium in Google Chrome prior to 51.0.2704.63 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.  |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-9651  | None | None | A missing check for whether a property of a JS object is private in V8 in Google Chrome prior to 55.0.2883.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15401 | None | None | A memory corruption bug in WebAssembly could lead to out of bounds read and write through V8 in WebAssembly in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15402 | None | None | Using an ID that can be controlled by a compromised renderer which allows any frame to overwrite the page_state of any other frame in the same process in Navigation in Google Chrome on Chrome OS prior to 62.0.3202.74 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15403 | None | None | Insufficient data validation in crash could lead to a command injection under chronos privileges in Networking in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15404 | None | None | An ability to process crash dumps under root privileges and inappropriate symlinks handling could lead to a local privilege escalation in Crash Reporting in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to perform privilege escalation via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15405 | None | None | Inappropriate symlink handling and a race condition in the stateful recovery feature implementation could lead to a persistence established by a malicious code running with root privileges in cryptohomed in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-15428 | None | None | Insufficient data validation in V8 builtins string generator could lead to out of bounds read and write access in V8 in Google Chrome prior to 62.0.3202.94 and allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16065 | None | None | A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.   |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16066 | None | None | A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16067 | None | None | A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16068 | None | None | Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16071 | None | None | A use after free in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16072 | None | None | A missing origin check related to HLS manifests in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass same origin policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16076 | None | None | Missing bounds check in PDFium in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16078 | None | None | Unsafe handling of credit card details in Autofill in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16079 | None | None | A race condition between permission prompts and navigations in Prompts in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16080 | None | None | A missing check for popup window handling in Fullscreen in Google Chrome on macOS prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16081 | None | None | Allowing the chrome.debugger API to run on file:// URLs in DevTools in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system without file access permission via a crafted Chrome Extension. |

|               |                    |                |      |      |   |
|---------------|--------------------|----------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16082 | None | None | An out of bounds read in Swiftshader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16083 | None | None | An out of bounds read in forward error correction code in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16084 | None | None | The default selected dialog button in CustomHandlers in Google Chrome prior to 69.0.3497.81 allowed a remote attacker who convinced the user to perform certain operations to open external programs via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16085 | None | None | A use after free in ResourceCoordinator in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16087 | None | None | Lack of proper state tracking in Permissions in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16088 | None | None | A missing check for JS-simulated input events in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to download arbitrary files with no user input via a crafted HTML page.                               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17457 | None | None | An object lifecycle issue in Blink could lead to a use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17458 | None | None | An improper update of the WebAssembly dispatch table in WebAssembly in Google Chrome prior to 69.0.3497.92 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17459 | None | None | Incorrect handling of clicks in the omnibox in Navigation in Google Chrome prior to 69.0.3497.92 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.                            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17461 | None | None | An out of bounds read in PDFium in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.  |

|               |                    |                |      |      |   |
|---------------|--------------------|----------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17470 | None | None | A heap buffer overflow in GPU in Google Chrome prior to 70.0.3538.67 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20065 | None | None | Handling of URI action in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to initiate potentially unsafe navigations without a user gesture via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20066 | None | None | Incorrect object lifecycle in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20067 | None | None | A renderer initiated back navigation was incorrectly allowed to cancel a browser initiated one in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20068 | None | None | Incorrect handling of 304 status codes in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20069 | None | None | Failure to prevent navigation to top frame to data URLs in Navigation in Google Chrome on iOS prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20070 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20071 | None | None | Insufficiently strict origin checks during JIT payment app installation in Payments in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to install a service worker for a domain that can host attacker controlled files via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6056  | None | None | Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6084  | None | None | Insufficiently sanitized distributed objects in Updater in Google Chrome on macOS prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via an executable file.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6091 | None | None | Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6093 | None | None | Insufficient origin checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6096 | None | None | A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6097 | None | None | Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6100 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6106 | None | None | An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6109 | None | None | readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6110 | None | None | Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to cause Chrome to execute scripts via a local non-HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6111 | None | None | An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6112 | None | None | Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.   |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6113 | None | None | Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6114 | None | None | Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6117 | None | None | Confusing settings in Autofill in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6120 | None | None | An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6123 | None | None | A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6124 | None | None | Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6126 | None | None | A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6127 | None | None | Early free of object in use in IndexedDB in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6133 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6135 | None | None | Lack of clearing the previous site before loading alerts from a new one in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6137 | None | None | CSS Paint API in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  |

|               |                    |               |      |      |   |
|---------------|--------------------|---------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6139 | None | None | Insufficient target checks on the chrome.debugger API in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6140 | None | None | Allowing the chrome.debugger API to attach to Web UI pages in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6141 | None | None | Insufficient validation of an image filter in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6143 | None | None | Insufficient validation in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6144 | None | None | Off-by-one error in PDFium in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6147 | None | None | Lack of secure text entry mode in Browser UI in Google Chrome on Mac prior to 67.0.3396.62 allowed a local attacker to obtain potentially sensitive information from process memory via a local process.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6151 | None | None | Bad cast in DevTools in Google Chrome on Win, Linux, Mac, Chrome OS prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6153 | None | None | A precision error in Skia in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6158 | None | None | A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6160 | None | None | JavaScript alert handling in Prompts in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6162 | None | None | Improper deserialization in WebGL in Google Chrome on Mac prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6163 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6164 | None | None | Insufficient origin checks for CSS content in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6165 | None | None | Incorrect handling of reloads in Navigation in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6166 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6167 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6169 | None | None | Lack of timeout on extension install prompt in Extensions in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to trigger installation of an unwanted extension via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6170 | None | None | A bad cast in PDFium in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6172 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6173 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6174 | None | None | Integer overflows in Swiftshader in Google Chrome prior to 68.0.3440.75 potentially allowed a remote attacker to execute arbitrary code via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6175 | None | None | Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6178 | None | None | Eliding from the wrong side in an infobar in DevTools in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to Hide Chrome Security UI via a crafted Chrome Extension.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6179 | None | None | Insufficient enforcement of file access permission in the activeTab case in Extensions in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5754 | None | None | Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5755 | None | None | Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5756 | None | None | Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5757 | None | None | An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5758 | None | None | Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5759 | None | None | Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.   |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5760 | None | None | Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5761 | None | None | Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5762 | None | None | Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5763 | None | None | Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5764 | None | None | Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5765 | None | None | An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5766 | None | None | Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5767 | None | None | Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5768 | None | None | DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension.           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5769 | None | None | Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5770 | None | None | Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5771 | None | None | An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5772 | None | None | Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5773 | None | None | Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5774 | None | None | Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file.                                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5775 | None | None | Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5776 | None | None | Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5777 | None | None | Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5778 | None | None | A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5779 | None | None | Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.  |

|               |                    |               |        |      |   |
|---------------|--------------------|---------------|--------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5780 | None   | None | Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5781 | None   | None | Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5782 | None   | None | Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5783 | None   | None | Missing URI encoding of untrusted input in DevTools in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform a Dangling Markup Injection attack via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5787 | HIGH   | 8.8  | Use-after-garbage-collection in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5788 | HIGH   | 8.8  | An integer overflow that leads to a use-after-free in Blink Storage in Google Chrome on Linux prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5789 | HIGH   | 8.8  | An integer overflow that leads to a use-after-free in WebMIDI in Google Chrome on Windows prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5790 | HIGH   | 8.8  | An integer overflow leading to an incorrect capacity of a buffer in JavaScript in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5791 | HIGH   | 8.8  | Inappropriate optimization in V8 in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5792 | HIGH   | 8.8  | Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5793 | MEDIUM | 6.5  | Insufficient policy enforcement in extensions in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to initiate the extensions installation user interface via a crafted HTML page.  |

|               |                    |               |        |      |  |
|---------------|--------------------|---------------|--------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5794 | MEDIUM | 6.5  | Incorrect handling of cancelled requests in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5795 | HIGH   | 8.8  | Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5796 | HIGH   | 7.5  | Data race in extensions guest view in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5798 | MEDIUM | 6.5  | Lack of correct bounds checking in Skia in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5799 | MEDIUM | 6.5  | Incorrect inheritance of a new document's policy in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5800 | MEDIUM | 6.5  | Insufficient policy enforcement in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5801 | MEDIUM | 6.5  | Incorrect eliding of URLs in Omnibox in Google Chrome on iOS prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5802 | MEDIUM | 6.5  | Incorrect handling of download origins in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5803 | MEDIUM | 6.5  | Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5804 | MEDIUM | 5.5  | Incorrect command line processing in Chrome in Google Chrome prior to 73.0.3683.75 allowed a local attacker to perform domain spoofing via a crafted domain name.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-7090 | None   | None | Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. |

|               |                    |                |      |      |  |
|---------------|--------------------|----------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2017-5028  | None | None | Insufficient data validation in V8 in Google Chrome prior to 56.0.2924.76 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16064 | None | None | Insufficient data validation in Extensions API in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16069 | None | None | Unintended floating-point error accumulation in SwiftShader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16070 | None | None | Integer overflows in Skia in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16073 | None | None | Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16074 | None | None | Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16075 | None | None | Insufficient file type enforcement in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain local file data via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16077 | None | None | Object lifecycle issue in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass content security policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-16086 | None | None | Insufficient policy enforcement in extensions API in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17460 | None | None | Insufficient data validation in filesystem URIs in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17478 | None | None | Incorrect array position calculations in V8 in Google Chrome prior to 70.0.3538.102 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.  |

|               |                    |                |      |      |   |
|---------------|--------------------|----------------|------|------|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-17479 | None | None | Incorrect object lifetime calculations in GPU code in Google Chrome prior to 70.0.3538.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-20073 | None | None | Use of extended attributes in downloads in Google Chrome prior to 72.0.3626.81 allowed a local attacker to read download URLs via the filesystem.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6118  | None | None | A double-eviction in the Incognito mode cache that lead to a user-after-free in cache in Google Chrome prior to 66.0.3359.139 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6121  | None | None | Insufficient validation of input in Blink in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to perform privilege escalation via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6128  | None | None | Incorrect URL parsing in WebKit in Google Chrome on iOS prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6129  | None | None | Out of bounds array access in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6130  | None | None | Incorrect handling of object lifetimes in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6131  | None | None | Object lifecycle issue in WebAssembly in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6132  | None | None | Uninitialized data in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6134  | None | None | Information leak in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass no-referrer policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6136  | None | None | Missing type check in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.  |

|               |                    |               |      |      |  |
|---------------|--------------------|---------------|------|------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6138 | None | None | Insufficient policy enforcement in Extensions API in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6142 | None | None | Array bounds check failure in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6145 | None | None | Insufficient data validation in HTML parser in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass same origin policy via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6148 | None | None | Incorrect implementation in Content Security Policy in Google Chrome prior to 67.0.3396.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6149 | None | None | Type confusion in JavaScript in Google Chrome prior to 67.0.3396.87 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6150 | None | None | Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6154 | None | None | Insufficient data validation in WebGL in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6155 | None | None | Incorrect handling of frames in the VP8 parser in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6156 | HIGH | 8.8  | Incorrect derivation of a packet length in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6157 | None | None | Type confusion in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6159 | None | None | Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.                           |

|               |                    |               |                         |               |  |
|---------------|--------------------|---------------|-------------------------|---------------|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6161 | None                    | None          | Insufficient policy enforcement in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6168 | None                    | None          | Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6171 | None                    | None          | Use after free in Bluetooth in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6176 | None                    | None          | Insufficient file type enforcement in Extensions API in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted Chrome Extension.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2018-6177 | None                    | None          | Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5784 | None                    | None          | Incorrect handling of deferred code in V8 in Google Chrome prior to 72.0.3626.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5785 | None                    | None          | Incorrect convexity calculations in Skia in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5786 | ['MEDIUM',<br>'MEDIUM'] | [6.5,<br>6.5] | Object lifetime issue in Blink in Google Chrome prior to 72.0.3626.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5805 | MEDIUM                  | 6.5           | Use-after-free in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5806 | HIGH                    | 8.8           | Integer overflow in ANGLE in Google Chrome on Windows prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5807 | HIGH                    | 8.8           | Object lifetime issue in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |

|               |                    |               |        |     |  |
|---------------|--------------------|---------------|--------|-----|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5808 | HIGH   | 8.8 | Use after free in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5809 | HIGH   | 8.8 | Use after free in file chooser in Google Chrome prior to 74.0.3729.108 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5810 | MEDIUM | 6.5 | Information leak in autofill in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5811 | HIGH   | 8.8 | Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.                                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5812 | MEDIUM | 6.5 | Inadequate security UI in iOS UI in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to perform domain spoofing via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5813 | HIGH   | 8.8 | Use after free in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5814 | MEDIUM | 6.5 | Insufficient policy enforcement in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                                      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5816 | HIGH   | 8.8 | Process lifetime issue in Chrome in Google Chrome on Android prior to 74.0.3729.108 allowed a remote attacker to potentially persist an exploited process via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5817 | HIGH   | 8.8 | Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5818 | MEDIUM | 6.5 | Uninitialized data in media in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.            |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5819 | HIGH   | 7.8 | Insufficient data validation in developer tools in Google Chrome on OS X prior to 74.0.3729.108 allowed a local attacker to execute arbitrary code via a crafted string copied to clipboard.       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5820 | HIGH   | 8.8 | Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  |

|               |                    |               |        |     |  |
|---------------|--------------------|---------------|--------|-----|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5821 | HIGH   | 8.8 | Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5822 | HIGH   | 8.8 | Inappropriate implementation in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.                        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5823 | MEDIUM | 5.4 | Insufficient policy enforcement in service workers in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.      |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5824 | HIGH   | 8.8 | Parameter passing error in media in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5827 | HIGH   | 8.8 | Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5828 | HIGH   | 8.8 | Object lifecycle issue in ServiceWorker in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5829 | HIGH   | 8.8 | Integer overflow in download manager in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5830 | MEDIUM | 6.5 | Insufficient policy enforcement in CORS in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5831 | HIGH   | 8.8 | Object lifecycle issue in V8 in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5832 | MEDIUM | 6.5 | Insufficient policy enforcement in XMLHttpRequest in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5833 | MEDIUM | 4.3 | Incorrect dialog box scoping in browser in Google Chrome on Android prior to 75.0.3770.80 allowed a remote attacker to display misleading security UI via a crafted HTML page.       |

|               |                    |               |          |     |  |
|---------------|--------------------|---------------|----------|-----|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5834 | MEDIUM   | 6.5 | Insufficient data validation in Blink in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to perform domain spoofing via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5835 | MEDIUM   | 6.5 | Object lifecycle issue in SwiftShader in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5836 | HIGH     | 8.8 | Heap buffer overflow in ANGLE in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5837 | MEDIUM   | 6.5 | Resource size information leakage in Blink in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5838 | MEDIUM   | 4.3 | Insufficient policy enforcement in extensions API in Google Chrome prior to 75.0.3770.80 allowed an attacker who convinced a user to install a malicious extension to bypass restrictions on file URIs via a crafted Chrome Extension.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5839 | MEDIUM   | 4.3 | Excessive data validation in URL parser in Google Chrome prior to 75.0.3770.80 allowed a remote attacker who convinced a user to input a URL to bypass website URL validation via a crafted URL.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-5840 | MEDIUM   | 4.3 | Incorrect security UI in popup blocker in Google Chrome on iOS prior to 75.0.3770.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5202 | CRITICAL | 9.1 | browser/extensions/api/dial/dial_registry.cc in Google Chrome before 54.0.2840.98 on macOS, before 54.0.2840.99 on Windows, and before 54.0.2840.100 on Linux neglects to copy a device ID before an erase() call, which causes the erase operation to access data that that erase operation will destroy. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1459 | MEDIUM   | 6.5 | The WebKit::WebPluginContainerImpl::handleEvent function in Google Chrome before Blink M11 allows an attacker to cause a denial of service (crash) via the htmlpluginelement.cpp plugin.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1460 | CRITICAL | 9.8 | WebKit in Google Chrome before Blink M11 contains a bad cast to RenderBlock when anonymous blocks are renderblocks.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1298 | HIGH     | 7.5 | An Integer Overflow exists in WebKit in Google Chrome before Blink M11 in the macOS WebCore::GraphicsContext::fillRect function.   |

|               |                    |                |          |     |   |
|---------------|--------------------|----------------|----------|-----|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2014-3180  | CRITICAL | 9.1 | In kernel/compat.c in the Linux kernel before 3.17, as used in Google Chrome OS and other products, there is a possible out-of-bounds read. restart_syscall uses uninitialized data when restarting compat_sys_nanosleep. NOTE: this is disputed because the code path is unreachable |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2808  | MEDIUM   | 6.5 | A stale layout root is set as an input element in WebKit in Google Chrome before Blink M13 when a child of a keygen with autofocus is accessed.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2353  | MEDIUM   | 6.5 | Use after free vulnerability in documentloader in WebKit in Google Chrome before Blink M13 in DocumentWriter::replaceDocument function.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2807  | MEDIUM   | 6.5 | Incorrect handling of timer information in Timer.cpp in WebKit in Google Chrome before Blink M13.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2336  | MEDIUM   | 6.5 | An issue exists in WebKit in Google Chrome before Blink M12. when clearing lists in AnimationControllerPrivate that signal when a hardware animation starts.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2337  | CRITICAL | 9.8 | A wrong type is used for a return value from strlen in WebKit in Google Chrome before Blink M12 on 64-bit platforms.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2335  | HIGH     | 7.5 | A double-free vulnerability exists in WebKit in Google Chrome before Blink M12 in the WebCore::CSSSelector function.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-2334  | MEDIUM   | 6.5 | Use after free vulnerability exists in WebKit in Google Chrome before Blink M12 in RenderLayer when removing elements with reflections.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1802  | MEDIUM   | 6.5 | WebKit in Google Chrome before Blink M11 and M12 does not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption).  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2011-1803  | MEDIUM   | 6.5 | An issue exists in third_party/WebKit/Source/WebCore/svg/animation/SVGSMILElement.h in WebKit in Google Chrome before Blink M11 and M12 when trying to access a removed smil element.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-5194  | CRITICAL | 9.8 | Unspecified vulnerabilities in Google Chrome before 54.0.2840.59.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2016-9652  | CRITICAL | 9.8 | Multiple unspecified vulnerabilities in Google Chrome before 55.0.2883.75.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13659 | MEDIUM   | 4.3 | IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.   |

|               |                    |                |        |     |   |
|---------------|--------------------|----------------|--------|-----|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13660 | MEDIUM | 5.3 | UI spoofing in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof notifications via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13661 | MEDIUM | 4.3 | UI spoofing in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof notifications via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13662 | MEDIUM | 6.5 | Insufficient policy enforcement in navigations in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13663 | MEDIUM | 4.3 | IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.                       |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13664 | MEDIUM | 6.5 | Insufficient policy enforcement in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13665 | MEDIUM | 6.5 | Insufficient filtering in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass multiple file download protection via a crafted HTML page.                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13666 | HIGH   | 7.4 | Information leak in storage in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13667 | MEDIUM | 4.3 | Inappropriate implementation in Omnibox in Google Chrome on iOS prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13668 | HIGH   | 7.4 | Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13669 | MEDIUM | 4.3 | Incorrect data validation in navigation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.        |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13670 | MEDIUM | 6.5 | Insufficient data validation in JavaScript in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13671 | MEDIUM | 4.3 | UI spoofing in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof security UI via a crafted HTML page.   |

|               |                    |                |        |     |  |
|---------------|--------------------|----------------|--------|-----|--|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13673 | HIGH   | 7.4 | Insufficient data validation in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13674 | MEDIUM | 4.3 | IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13675 | MEDIUM | 4.3 | Insufficient data validation in extensions in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to disable extensions via a crafted HTML page.                           |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13676 | MEDIUM | 4.3 | Insufficient policy enforcement in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.                     |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13677 | MEDIUM | 6.5 | Insufficient policy enforcement in site isolation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13678 | MEDIUM | 6.5 | Incorrect data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.                          |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13679 | LOW    | 3.3 | Insufficient policy enforcement in PDFium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to show print dialogs via a crafted PDF file.                             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13680 | MEDIUM | 5.3 | Inappropriate implementation in TLS in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof client IP address to websites via crafted TLS connections.             |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13681 | MEDIUM | 4.3 | Insufficient data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass download restrictions via a crafted HTML page.                  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13682 | HIGH   | 8.8 | Insufficient policy enforcement in external protocol handling in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13683 | MEDIUM | 6.5 | Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.               |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13684 | MEDIUM | 5.3 | Inappropriate implementation in JavaScript in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                       |

|               |                    |                |        |     |   |
|---------------|--------------------|----------------|--------|-----|---|
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13685 | HIGH   | 8.8 | Use after free in sharing view in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13686 | HIGH   | 8.8 | Use after free in offline mode in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                   |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13687 | HIGH   | 8.8 | Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13688 | HIGH   | 8.8 | Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13691 | MEDIUM | 4.3 | Insufficient validation of untrusted input in navigation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13692 | HIGH   | 8.8 | Insufficient policy enforcement in reader mode in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.                                 |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13693 | HIGH   | 8.8 | Use after free in IndexedDB in Google Chrome prior to 77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.         |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13694 | HIGH   | 8.8 | Use after free in WebRTC in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13695 | HIGH   | 8.8 | Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                              |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13696 | HIGH   | 8.8 | Use after free in JavaScript in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.                                    |
| Google Chrome | 135.0.704<br>9.116 | CVE-2019-13697 | MEDIUM | 6.5 | Insufficient policy enforcement in performance APIs in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to leak cross-origin data via a crafted HTML page.                          |

|                                   |                    |                |        |      |  |
|-----------------------------------|--------------------|----------------|--------|------|--|
| Google Chrome                     | 135.0.704<br>9.116 | CVE-2019-13698 | HIGH   | 8.8  | Out of bounds memory access in JavaScript in Google Chrome prior to 73.0.3683.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome                     | 135.0.704<br>9.116 | CVE-2019-13699 | HIGH   | 8.8  | Use after free in media in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.  |
| Google Chrome                     | 135.0.704<br>9.116 | CVE-2019-13700 | HIGH   | 8.8  | Out of bounds memory access in the gamepad API in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.   |
| Google Chrome                     | 135.0.704<br>9.116 | CVE-2019-13701 | MEDIUM | 4.3  | Incorrect implementation in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  |
| Google Chrome                     | 135.0.704<br>9.116 | CVE-2019-13702 | HIGH   | 7.8  | Inappropriate implementation in installer in Google Chrome on Windows prior to 78.0.3904.70 allowed a local attacker to perform privilege escalation via a crafted executable.   |
| Intel(R) LMS                      | 1.0.0.0            | CVE-2020-8704  | MEDIUM | 6.4  | Race condition in a subsystem in the Intel(R) LMS versions before 2039.1.0.0 may allow a privileged user to potentially enable escalation of privilege via local access.   |
| Intel(R) Management Engine Driver | 1.0.0.0            | CVE-2019-11097 | HIGH   | 7.8  | Improper directory permissions in the installer for Intel(R) Management Engine Consumer Driver for Windows before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access. |
| Intel(R) Management Engine Driver | 1.0.0.0            | CVE-2021-33087 | MEDIUM | 5.5  | Improper authentication in the installer for the Intel(R) NUC M15 Laptop Kit Management Engine driver pack before version 15.0.10.1508 may allow an authenticated user to potentially enable denial of service via local access.   |
| McAfee                            | 1.29.162.1         | CVE-2000-0119  | None   | None | The default configurations for McAfee Virus Scan and Norton Anti-Virus virus checkers do not check files in the RECYCLED folder that is used by the Windows Recycle Bin utility, which allows attackers to store malicious code without detection.   |
| McAfee                            | 1.29.162.1         | CVE-2000-0502  | None   | None | McAfee VirusScan 4.03 does not properly restrict access to the alert text file before it is sent to the Central Alert Server, which allows local users to modify alerts in an arbitrary fashion.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2000-1128 | None | None | The default configuration of McAfee VirusScan 4.5 does not quote the ImagePath variable, which improperly sets the search path and allows local users to place a Trojan horse "common.exe" program in the C:\Program Files directory.   |
| McAfee | 1.29.162.1 | CVE-2000-1129 | None | None | McAfee WebShield SMTP 4.5 allows remote attackers to cause a denial of service via a malformed recipient field.   |
| McAfee | 1.29.162.1 | CVE-2000-1130 | None | None | McAfee WebShield SMTP 4.5 allows remote attackers to bypass email content filtering rules by including Extended ASCII characters in name of the attachment.   |
| McAfee | 1.29.162.1 | CVE-2001-1144 | None | None | Directory traversal vulnerability in McAfee ASaP VirusScan agent 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the HTTP request.  |
| McAfee | 1.29.162.1 | CVE-2001-0612 | None | None | McAfee Remote Desktop 3.0 and earlier allows remote attackers to cause a denial of service (crash) via a large number of packets to port 5045.  |
| McAfee | 1.29.162.1 | CVE-2002-2282 | None | None | McAfee VirusScan 4.5.1, when the WebScanX.exe module is enabled, searches for particular DLLs from the user's home directory, even when browsing the local hard drive, which allows local users to run arbitrary code via malicious versions of those DLLs.   |
| McAfee | 1.29.162.1 | CVE-2002-0690 | None | None | Format string vulnerability in McAfee Security ePolicy Orchestrator (ePO) 2.5.1 allows remote attackers to execute arbitrary code via an HTTP GET request with a URI containing format strings.   |
| McAfee | 1.29.162.1 | CVE-2003-0148 | None | None | The default installation of MSDE via McAfee ePolicy Orchestrator 2.0 through 3.0 allows attackers to execute arbitrary code via a series of steps that (1) obtain the database administrator username and encrypted password in a configuration file from the ePO server using a certain request, (2) crack the password due to weak cryptography, and (3) use the password to pass commands through xp_cmdshell. |
| McAfee | 1.29.162.1 | CVE-2003-0149 | None | None | Heap-based buffer overflow in ePO agent for McAfee ePolicy Orchestrator 2.0, 2.5, and 2.5.1 allows remote attackers to execute arbitrary code via a POST request containing long parameters.  |
| McAfee | 1.29.162.1 | CVE-2003-0610 | None | None | Directory traversal vulnerability in ePO agent for McAfee ePolicy Orchestrator 3.0 allows remote attackers to read arbitrary files via a certain HTTP request.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2003-0616 | None | None | Format string vulnerability in ePO service for McAfee ePolicy Orchestrator 2.0, 2.5, and 2.5.1 allows remote attackers to execute arbitrary code via a POST request with format strings in the computerlist parameter, which are used when logging a failed name resolution. |
| McAfee | 1.29.162.1 | CVE-2004-0095 | None | None | McAfee ePolicy Orchestrator agent allows remote attackers to cause a denial of service (memory consumption and crash) and possibly execute arbitrary code via an HTTP POST request with an invalid Content-Length value, possibly triggering a buffer overflow.              |
| McAfee | 1.29.162.1 | CVE-2004-0038 | None | None | McAfee ePolicy Orchestrator (ePO) 2.5.1 Patch 13 and 3.0 SP2a Patch 3 allows remote attackers to execute arbitrary commands via certain HTTP POST requests to the spipe/file handler on ePO TCP port 81.   |
| McAfee | 1.29.162.1 | CVE-2004-0831 | None | None | McAfee VirusScan 4.5.1 does not drop SYSTEM privileges before allowing users to browse for files via the "System Scan" properties of the System Tray applet, which could allow local users to gain privileges.   |
| McAfee | 1.29.162.1 | CVE-2004-1906 | None | None | Mcafee FreeScan allows remote attackers to cause a denial of service and possibly arbitrary code via a long string in the ScanParam property of a COM object, which may trigger a buffer overflow.   |
| McAfee | 1.29.162.1 | CVE-2004-1908 | None | None | McFreeScan.CoMcFreeScan.1 ActiveX object in Mcafee FreeScan allows remote attackers to obtain sensitive information via the GetSpecialFolderLocation function with certain parameters.   |
| McAfee | 1.29.162.1 | CVE-2004-2635 | None | None | An ActiveX control for McAfee Security Installer Control System 4.0.0.81 allows remote attackers to access the Windows registry via web pages that use the control's RegQueryValue() method.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2004-1094 | None | None | Buffer overflow in InnerMedia DynaZip DUNZIP32.dll file version 5.00.03 and earlier allows remote attackers to execute arbitrary code via a ZIP file containing a file with a long filename, as demonstrated using (1) a .rjs (skin) file in RealPlayer 10 through RealPlayer 10.5 (6.0.12.1053), RealOne Player 1 and 2, (2) the Restore Backup function in CheckMark Software Payroll 2004/2005 3.9.6 and earlier, (3) CheckMark MultiLedger before 7.0.2, (4) dtSearch 6.x and 7.x, (5) mcupdmgr.exe and mghtml.exe in McAfee VirusScan 10 Build 10.0.21 and earlier, (6) IBM Lotus Notes before 6.5.5, and other products. NOTE: it is unclear whether this is the same vulnerability as CVE-2004-0575, although the data manipulations are the same. |
| McAfee | 1.29.162.1 | CVE-2004-0932 | None | None | McAfee Anti-Virus Engine DATS drivers before 4398 released on Oct 13th 2004 and DATS Driver before 4397 October 6th 2004 allows remote attackers to bypass antivirus protection via a compressed file with both local and global headers set to zero, which does not prevent the compressed file from being opened on a target system.  |
| McAfee | 1.29.162.1 | CVE-2005-1107 | None | None | McAfee Internet Security Suite 2005 uses insecure default ACLs for installed files, which allows local users to gain privileges or disable protection by modifying certain files.   |
| McAfee | 1.29.162.1 | CVE-2005-0643 | None | None | Buffer overflow in McAfee Scan Engine 4320 with DAT version before 4357 allows remote attackers to execute arbitrary code via crafted LHA files.  |
| McAfee | 1.29.162.1 | CVE-2005-0644 | None | None | Buffer overflow in McAfee Scan Engine 4320 with DAT version before 4436 allows remote attackers to execute arbitrary code via a malformed LHA file with a type 2 header file name field, a variant of CVE-2005-0643.  |
| McAfee | 1.29.162.1 | CVE-2005-2186 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in McAfee IntruShield Security Management System allow remote authenticated users to inject arbitrary web script or HTML via the (1) thirdMenuName or (2) resourceName parameter to SystemEvent.jsp.  |
| McAfee | 1.29.162.1 | CVE-2005-2187 | None | None | McAfee IntruShield Security Management System allows remote authenticated users to access the "Generate Reports" feature and modify alerts by setting the Access option to true, as demonstrated using the (1) fullAccess or (2) fullAccessRight parameter in reports-column-center.jsp, or (3) fullAccess parameter to SystemEvent.jsp.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2005-2188 | None | None | McAfee IntruShield Security Management System obtains the user ID from the URL, which allows remote attackers to guess the Manager account and possibly gain privileges via a brute force attack.  |
| McAfee | 1.29.162.1 | CVE-2005-3215 | None | None | Multiple interpretation error in unspecified versions of McAfee Antivirus allows remote attackers to bypass virus detection via a malicious executable in a specially crafted RAR file with malformed central and local headers, which can still be opened by products such as Winrar and PowerZip, even though they are rejected as corrupted by Winzip and BitZipper.  |
| McAfee | 1.29.162.1 | CVE-2005-3377 | None | None | Multiple interpretation error in (1) McAfee Internet Security Suite 7.1.5 version 9.1.08 with the 4.4.00 engine and (2) McAfee Corporate 8.0.0 patch 10 with the 4400 engine allows remote attackers to bypass virus scanning via a file such as BAT, HTML, and EML with an "MZ" magic byte sequence which is normally associated with EXE, which causes the file to be treated as a safe type that could still be executed as a dangerous file type by applications on the end system, as demonstrated by a "triple headed" program that contains EXE, EML, and HTML content, aka the "magic byte bug." |
| McAfee | 1.29.162.1 | CVE-2005-3657 | None | None | The ActiveX control in MCINSCTL.DLL for McAfee VirusScan Security Center does not use the IObjectSafetySiteLock API to restrict access to required domains, which allows remote attackers to create or append to arbitrary files via the StartLog and AddLog methods in the MCINSTALL.McLog object.  |
| McAfee | 1.29.162.1 | CVE-2005-4505 | None | None | Unquoted Windows search path vulnerability in McAfee VirusScan Enterprise 8.0i (patch 11) and CMA 3.5 (patch 5) might allow local users to gain privileges via a malicious "program.exe" file in the C: folder, which is run by naPrdMgr.exe when it attempts to execute EntVUtil.EXE under an unquoted "Program Files" path.  |
| McAfee | 1.29.162.1 | CVE-2006-0982 | None | None | The on-access scanner for McAfee Virex 7.7 for Macintosh, in some circumstances, might not activate when malicious content is accessed from the web browser, and might not prevent the content from being saved, which allows remote attackers to bypass virus protection, as demonstrated using the EICAR test file.  |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2006-0559 | None | None | Format string vulnerability in the SMTP server for McAfee WebShield 4.5 MR2 and earlier allows remote attackers to execute arbitrary code via format strings in the domain name portion of a destination address, which are not properly handled when a bounce message is constructed.  |
| McAfee | 1.29.162.1 | CVE-2006-3575 | None | None | Unknown vulnerability in the Buffer Overflow Protection in McAfee VirusScan Enterprise 8.0.0 allows local users to cause a denial of service (unstable operation) via a long string in the (1) "Process name", (2) "Module name", or (3) "API name" fields.   |
| McAfee | 1.29.162.1 | CVE-2006-3623 | None | None | Directory traversal vulnerability in Framework Service component in McAfee ePolicy Orchestrator agent 3.5.0.x and earlier allows remote attackers to create arbitrary files via a .. (dot dot) in the directory and filename in a PropsResponse (PackageType) request.  |
| McAfee | 1.29.162.1 | CVE-2006-3961 | None | None | Buffer overflow in McSubMgr ActiveX control (mcsbmgr.dll) in McAfee Security Center 6.0.23 for Internet Security Suite 2006, Wireless Home Network Security, Personal Firewall Plus, VirusScan, Privacy Service, SpamKiller, AntiSpyware, and QuickClean allows remote user-assisted attackers to execute arbitrary commands via long string parameters, which are later used in vsprintf.    |
| McAfee | 1.29.162.1 | CVE-2006-4886 | None | None | The VirusScan On-Access Scan component in McAfee VirusScan Enterprise 7.1.0 and Scan Engine 4.4.00 allows local privileged users to bypass security restrictions and disable the On-Access Scan option by opening the program via the task bar and quickly clicking the Disable button, possibly due to an interface-related race condition.  |
| McAfee | 1.29.162.1 | CVE-2006-5156 | None | None | Buffer overflow in McAfee ePolicy Orchestrator before 3.5.0.720 and ProtectionPilot before 1.1.1.126 allows remote attackers to execute arbitrary code via a request to /spipe/pkg/ with a long source header.  |
| McAfee | 1.29.162.1 | CVE-2006-5417 | None | None | McAfee Network Agent (mcnasvc.exe) 1.0.178.0, as used by multiple McAfee products possibly including Internet Security Suite, Personal Firewall Plus, and VirusScan, allows remote attackers to cause a denial of service (agent crash) via a long packet, possibly because of an invalid string position field value. NOTE: some of these details are obtained from third party information. |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2006-6474 | None | None | Untrusted search path vulnerability in McAfee VirusScan for Linux 4510e and earlier includes the current working directory in the DT_RPATH environment variable, which allows local users to load arbitrary ELF DSO libraries and execute arbitrary code by installing malicious libraries in that directory.  |
| McAfee | 1.29.162.1 | CVE-2006-6707 | None | None | Stack-based buffer overflow in the NeoTraceExplorer.NeoTraceLoader ActiveX control (NeoTraceExplorer.dll) in NeoTrace Express 3.25 and NeoTrace Pro (aka McAfee Visual Trace) 3.25 allows remote attackers to execute arbitrary code via a long argument string to the TraceTarget method. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.  |
| McAfee | 1.29.162.1 | CVE-2007-1226 | None | None | McAfee VirusScan for Mac (Virex) before 7.7 patch 1 has weak permissions (0666) for /Library/Application Support/Virex/VShieldExclude.txt, which allows local users to reconfigure Virex to skip scanning of arbitrary files.  |
| McAfee | 1.29.162.1 | CVE-2007-1227 | None | None | VShieldCheck in McAfee VirusScan for Mac (Virex) before 7.7 patch 1 allow local users to change permissions of arbitrary files via a symlink attack on /Library/Application Support/Virex/VShieldExclude.txt, as demonstrated by symlinking to the root crontab file to execute arbitrary commands.  |
| McAfee | 1.29.162.1 | CVE-2007-1498 | None | None | Multiple stack-based buffer overflows in the SiteManager.SiteMgr.1 ActiveX control (SiteManager.dll) in the ePO management console in McAfee ePolicy Orchestrator (ePO) before 3.6.1 Patch 1 and ProtectionPilot (PRP) before 1.5.0 HotFix allow remote attackers to execute arbitrary code via a long argument to the (1) ExportSiteList and (2) VerifyPackageCatalog functions, and (3) unspecified vectors involving a swprintf function call.  |
| McAfee | 1.29.162.1 | CVE-2007-1538 | None | None | McAfee VirusScan Enterprise 8.5.0.i uses insecure permissions for certain Windows Registry keys, which allows local users to bypass local password protection via the UIP value in (1) HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\DesktopProtection or (2) HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\VirusScan Enterprise\CurrentVersion. NOTE: this issue has been disputed by third-party researchers, stating that the default permissions for HKEY_LOCAL_MACHINE\SOFTWARE does not allow for write access and the product does not modify the inherited permissions. There might be an interaction error with another product |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2007-2151 | None | None | The administration server in McAfee e-Business Server before 8.1.1 and 8.5.x before 8.5.2 allows remote attackers to cause a denial of service (service crash) via a large length value in a malformed authentication packet, which triggers a heap over-read.                                |
| McAfee | 1.29.162.1 | CVE-2007-2152 | None | None | Buffer overflow in the On-Access Scanner in McAfee VirusScan Enterprise before 8.0i Patch 12 allows user-assisted remote attackers to execute arbitrary code via a long filename containing multi-byte (Unicode) characters.  |
| McAfee | 1.29.162.1 | CVE-2007-2584 | None | None | Buffer overflow in the IsOldAppInstalled function in the McSubMgr.McSubMgr Subscription Manager ActiveX control (MCSUBMGR.DLL) in McAfee SecurityCenter before 6.0.25 and 7.x before 7.2.147 allows remote attackers to execute arbitrary code via a crafted argument.                        |
| McAfee | 1.29.162.1 | CVE-2006-5271 | None | None | Integer underflow in McAfee ePolicy Orchestrator 3.5 through 3.6.1, ProtectionPilot 1.1.1 and 1.5, and Common Management Agent (CMA) 3.6.0.453 and earlier allows remote attackers to execute arbitrary code via a crafted UDP packet, which causes stack corruption.                         |
| McAfee | 1.29.162.1 | CVE-2006-5272 | None | None | Stack-based buffer overflow in McAfee ePolicy Orchestrator 3.5 through 3.6.1, ProtectionPilot 1.1.1 and 1.5, and Common Management Agent (CMA) 3.6.0.453 and earlier allows remote attackers to execute arbitrary code via a crafted ping packet.   |
| McAfee | 1.29.162.1 | CVE-2006-5273 | None | None | Heap-based buffer overflow in McAfee ePolicy Orchestrator 3.5 through 3.6.1, ProtectionPilot 1.1.1 and 1.5, and Common Management Agent (CMA) 3.5.5.438 through 3.6.0.453 allows remote attackers to execute arbitrary code via a crafted packet.   |
| McAfee | 1.29.162.1 | CVE-2006-5274 | None | None | Integer overflow in McAfee ePolicy Orchestrator 3.5 through 3.6.1, ProtectionPilot 1.1.1 and 1.5, and Common Management Agent (CMA) 3.5.5.438 allows remote attackers to cause a denial of service (CMA Framework service crash) and possibly execute arbitrary code via unspecified vectors. |
| McAfee | 1.29.162.1 | CVE-2007-2957 | None | None | Integer overflow in McAfee E-Business Server before 8.5.3 for Solaris, and before 8.1.2 for Linux, HP-UX, and AIX, allows remote attackers to execute arbitrary code via a large length value in an authentication packet, which results in a heap-based buffer overflow.                     |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2008-0127 | None | None | The administration interface in McAfee E-Business Server 8.5.2 and earlier allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a long initial authentication packet.  |
| McAfee | 1.29.162.1 | CVE-2008-1357 | None | None | Format string vulnerability in the logDetail function of applib.dll in McAfee Common Management Agent (CMA) 3.6.0.574 (Patch 3) and earlier, as used in ePolicy Orchestrator 4.0.0 build 1015, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via format string specifiers in a sender field in an AgentWakeup request to UDP port 8082. NOTE: this issue only exists when the debug level is 8.  |
| McAfee | 1.29.162.1 | CVE-2008-1855 | None | None | FrameworkService.exe in McAfee Common Management Agent (CMA) 3.6.0.574 Patch 3 and earlier, as used by ePolicy Orchestrator (ePO) and ProtectionPilot (PrP), allows remote attackers to corrupt memory and cause a denial of service (CMA Framework service crash) via a long invalid method in requests for the /spin//AVClient//AVClient.csp URI, a different vulnerability than CVE-2006-5274.   |
| McAfee | 1.29.162.1 | CVE-2008-3605 | None | None | Unspecified vulnerability in McAfee Encrypted USB Manager 3.1.0.0, when the Re-use Threshold for passwords is nonzero, allows remote attackers to conduct offline brute force attacks via unknown vectors.  |
| McAfee | 1.29.162.1 | CVE-2008-5257 | None | None | webseald in WebSEAL 6.0.0.17 in IBM Tivoli Access Manager for e-business allows remote attackers to cause a denial of service (crash or hang) via HTTP requests, as demonstrated by a McAfee vulnerability scan.  |
| McAfee | 1.29.162.1 | CVE-2009-1348 | None | None | The AV engine before DAT 5600 in McAfee VirusScan, Total Protection, Internet Security, SecurityShield for Microsoft ISA Server, Security for Microsoft Sharepoint, Security for Email Servers, Email Gateway, and Active Virus Defense allows remote attackers to bypass virus detection via (1) an invalid Headflags field in a malformed RAR archive, (2) an invalid Packsize field in a malformed RAR archive, or (3) an invalid Filelength field in a malformed ZIP archive. |
| McAfee | 1.29.162.1 | CVE-2009-1491 | None | None | McAfee GroupShield for Microsoft Exchange on Exchange Server 2000, and possibly other anti-virus or anti-spam products from McAfee or other vendors, does not scan X- headers for malicious content, which allows remote attackers to bypass virus detection via a crafted message, as demonstrated by a message with an X-Testing header and no message body.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2008-7020 | None | None | McAfee SafeBoot Device Encryption 4 build 4750 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.   |
| McAfee | 1.29.162.1 | CVE-2009-3339 | None | None | Unspecified vulnerability in McAfee Email and Web Security Appliance 5.1 VMtrial allows remote attackers to read arbitrary files via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.9 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. |
| McAfee | 1.29.162.1 | CVE-2009-3565 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in intruvert/jsp/module/Login.jsp in McAfee IntruShield Network Security Manager (NSM) before 5.1.11.6 allow remote attackers to inject arbitrary web script or HTML via the (1) iaction or (2) node parameter.  |
| McAfee | 1.29.162.1 | CVE-2009-3566 | None | None | McAfee IntruShield Network Security Manager (NSM) before 5.1.11.8.1 does not include the HTTPOnly flag in the Set-Cookie header for the session identifier, which allows remote attackers to hijack a session by leveraging a cross-site scripting (XSS) vulnerability.  |
| McAfee | 1.29.162.1 | CVE-2010-2116 | None | None | The web interface in McAfee Email Gateway (formerly IronMail) 6.7.1 allows remote authenticated users, with only Read privileges, to gain Write privileges to modify configuration via the save action in a direct request to admin/systemWebAdminConfig.do.   |
| McAfee | 1.29.162.1 | CVE-2010-2290 | None | None | Cross-site scripting (XSS) vulnerability in cgi-bin/cgix/help in McAfee Unified Threat Management (UTM) Firewall (formerly SnapGear) firmware 3.0.0 through 4.0.6 allows remote attackers to inject arbitrary web script or HTML via the page parameter.   |
| McAfee | 1.29.162.1 | CVE-2011-3006 | None | None | The MyAsUtil ActiveX control in MyAsUtil5.2.0.603.dll in McAfee SaaS Endpoint Protection 5.2.1 and earlier allows remote attackers to bypass the MyASUtil.SecureObjectFactory.Create SecureObject domain execution policy using a cross-site scripting (XSS) attack, execute arbitrary code using the MyASUtil.InstallInfo.RunUserProgram function, and possibly conduct other unspecified attacks.  |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2011-3007 | None | None | The myCIOScn ActiveX control (myCIOScn.dll) in McAfee SaaS Endpoint Protection 5.2.1 and earlier allows remote attackers to write to arbitrary files by specifying an arbitrary filename in the MyCioScan.Scan.ReportFile parameter, as demonstrated by injecting script into a log file and executing arbitrary code using the MyCioScan.Scan.Start method.  |
| McAfee | 1.29.162.1 | CVE-2012-1425 | None | None | The TAR file parser in Avira AntiVir 7.11.1.163, Antiy Labs AVL SDK 2.0.3.7, Quick Heal (aka Cat QuickHeal) 11.00, Emsisoft Anti-Malware 5.1.0.1, Fortinet Antivirus 4.2.254.0, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Jiangmin Antivirus 13.0.900, Kaspersky Anti-Virus 7.0.0.125, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, NOD32 Antivirus 5795, Norman Antivirus 6.06.12, PC Tools AntiVirus 7.0.3.5, AVEngine 20101.3.0.103 in Symantec Endpoint Protection 11, Trend Micro AntiVirus 9.120.0.1004, and Trend Micro HouseCall 9.120.0.1004 allows remote attackers to bypass malware detection via a POSIX TAR file with an initial \50\4B\03\04 character sequence. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different TAR parser implementations. |
| McAfee | 1.29.162.1 | CVE-2012-1429 | None | None | The ELF file parser in Bitdefender 7.2, Comodo Antivirus 7424, Emsisoft Anti-Malware 5.1.0.1, eSafe 7.0.17.0, F-Secure Anti-Virus 9.0.16160.0, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, and nProtect Anti-Virus 2011-01-17.01 allows remote attackers to bypass malware detection via an ELF file with a ustar character sequence at a certain location. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations.  |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2012-1430 | None | None | The ELF file parser in Bitdefender 7.2, Comodo Antivirus 7424, eSafe 7.0.17.0, F-Secure Anti-Virus 9.0.16160.0, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, nProtect Anti-Virus 2011-01-17.01, Sophos Anti-Virus 4.61.0, and Rising Antivirus 22.83.00.03 allows remote attackers to bypass malware detection via an ELF file with a \19\04\00\10 character sequence at a certain location. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations.   |
| McAfee | 1.29.162.1 | CVE-2012-1431 | None | None | The ELF file parser in Bitdefender 7.2, Command Antivirus 5.2.11.5, Comodo Antivirus 7424, eSafe 7.0.17.0, F-Prot Antivirus 4.6.2.117, F-Secure Anti-Virus 9.0.16160.0, McAfee Gateway (formerly Webwasher) 2010.1C, nProtect Anti-Virus 2011-01-17.01, Sophos Anti-Virus 4.61.0, and Rising Antivirus 22.83.00.03 allows remote attackers to bypass malware detection via an ELF file with a \4a\46\49\46 character sequence at a certain location. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations.                                       |
| McAfee | 1.29.162.1 | CVE-2012-1442 | None | None | The ELF file parser in Quick Heal (aka Cat QuickHeal) 11.00, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, eSafe 7.0.17.0, Kaspersky Anti-Virus 7.0.0.125, F-Secure Anti-Virus 9.0.16160.0, Sophos Anti-Virus 4.61.0, Antiy Labs AVL SDK 2.0.3.7, Rising Antivirus 22.83.00.03, Fortinet Antivirus 4.2.254.0, and Panda Antivirus 10.0.2.7 allows remote attackers to bypass malware detection via an ELF file with a modified class field. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations. |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2012-1443 | None | None | The RAR file parser in ClamAV 0.96.4, Rising Antivirus 22.83.00.03, Quick Heal (aka Cat QuickHeal) 11.00, G Data AntiVirus 21, AVEngine 20101.3.0.103 in Symantec Endpoint Protection 11, Command Antivirus 5.2.11.5, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Emsisoft Anti-Malware 5.1.0.1, PC Tools AntiVirus 7.0.3.5, F-Prot Antivirus 4.6.2.117, VirusBuster 13.6.151.0, Fortinet Antivirus 4.2.254.0, Antiy Labs AVL SDK 2.0.3.7, K7 AntiVirus 9.77.3565, Trend Micro HouseCall 9.120.0.1004, Kaspersky Anti-Virus 7.0.0.125, Jiangmin Antivirus 13.0.900, Antimalware Engine 1.1.6402.0 in Microsoft Security Essentials 2.0, Sophos Anti-Virus 4.61.0, NOD32 Antivirus 5795, Avira AntiVir 7.11.1.163, Norman Antivirus 6.06.12, McAfee Anti-Virus Scanning Engine 5.400.0.1158, Panda Antivirus 10.0.2.7, McAfee Gateway (formerly Webwasher) 2010.1C, Trend Micro AntiVirus 9.120.0.1004, Comodo Antivirus 7424, Bitdefender 7.2, eSafe 7.0.17.0, F-Secure Anti-Virus 9.0.16160.0, nProtect Anti-Virus 2011... |
| McAfee | 1.29.162.1 | CVE-2012-1446 | None | None | The ELF file parser in Quick Heal (aka Cat QuickHeal) 11.00, McAfee Anti-Virus Scanning Engine 5.400.0.1158, AVEngine 20101.3.0.103 in Symantec Endpoint Protection 11, Norman Antivirus 6.06.12, eSafe 7.0.17.0, Kaspersky Anti-Virus 7.0.0.125, McAfee Gateway (formerly Webwasher) 2010.1C, Sophos Anti-Virus 4.61.0, CA eTrust Vet Antivirus 36.1.8511, Antiy Labs AVL SDK 2.0.3.7, PC Tools AntiVirus 7.0.3.5, Rising Antivirus 22.83.00.03, Fortinet Antivirus 4.2.254.0, and Panda Antivirus 10.0.2.7 allows remote attackers to bypass malware detection via an ELF file with a modified encoding field. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2012-1453 | None | None | The CAB file parser in Dr.Web 5.0.2.03300, Trend Micro HouseCall 9.120.0.1004, Kaspersky Anti-Virus 7.0.0.125, Sophos Anti-Virus 4.61.0, Trend Micro AntiVirus 9.120.0.1004, McAfee Gateway (formerly Webwasher) 2010.1C, Emsisoft Anti-Malware 5.1.0.1, CA eTrust Vet Antivirus 36.1.8511, Antiy Labs AVL SDK 2.0.3.7, Antimalware Engine 1.1.6402.0 in Microsoft Security Essentials 2.0, Rising Antivirus 22.83.00.03, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Fortinet Antivirus 4.2.254.0, and Panda Antivirus 10.0.2.7 allows remote attackers to bypass malware detection via a CAB file with a modified coffFiles field. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different CAB parser implementations.   |
| McAfee | 1.29.162.1 | CVE-2012-1454 | None | None | The ELF file parser in Dr.Web 5.0.2.03300, eSafe 7.0.17.0, McAfee Gateway (formerly Webwasher) 2010.1C, Rising Antivirus 22.83.00.03, Fortinet Antivirus 4.2.254.0, and Panda Antivirus 10.0.2.7 allows remote attackers to bypass malware detection via an ELF file with a modified ei_version field. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations.  |
| McAfee | 1.29.162.1 | CVE-2012-1456 | None | None | The TAR file parser in AVG Anti-Virus 10.0.0.1190, Quick Heal (aka Cat QuickHeal) 11.00, Comodo Antivirus 7424, Emsisoft Anti-Malware 5.1.0.1, eSafe 7.0.17.0, F-Prot Antivirus 4.6.2.117, Fortinet Antivirus 4.2.254.0, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Jiangmin Antivirus 13.0.900, Kaspersky Anti-Virus 7.0.0.125, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, NOD32 Antivirus 5795, Norman Antivirus 6.06.12, Panda Antivirus 10.0.2.7, Rising Antivirus 22.83.00.03, Sophos Anti-Virus 4.61.0, AVEngine 20101.3.0.103 in Symantec Endpoint Protection 11, Trend Micro AntiVirus 9.120.0.1004, and Trend Micro HouseCall 9.120.0.1004 allows remote attackers to bypass malware detection via a TAR file with an appended ZIP file. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different TAR parser implementations. |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2012-1457 | None | None | The TAR file parser in Avira AntiVir 7.11.1.163, Antiy Labs AVL SDK 2.0.3.7, avast! Antivirus 4.8.1351.0 and 5.0.677.0, AVG Anti-Virus 10.0.0.1190, Bitdefender 7.2, Quick Heal (aka Cat QuickHeal) 11.00, ClamAV 0.96.4, Command Antivirus 5.2.11.5, Emsisoft Anti-Malware 5.1.0.1, eSafe 7.0.17.0, F-Prot Antivirus 4.6.2.117, G Data AntiVirus 21, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Jiangmin Antivirus 13.0.900, K7 AntiVirus 9.77.3565, Kaspersky Anti-Virus 7.0.0.125, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, Antimalware Engine 1.1.6402.0 in Microsoft Security Essentials 2.0, NOD32 Antivirus 5795, Norman Antivirus 6.06.12, PC Tools AntiVirus 7.0.3.5, Rising Antivirus 22.83.00.03, AVEngine 20101.3.0.103 in Symantec Endpoint Protection 11, Trend Micro AntiVirus 9.120.0.1004, Trend Micro HouseCall 9.120.0.1004, VBA32 3.12.14.2, and VirusBuster 13.6.151.0 allows remote attackers to bypass malware detection via a TAR archive e... |
| McAfee | 1.29.162.1 | CVE-2012-1459 | None | None | The TAR file parser in AhnLab V3 Internet Security 2011.01.18.00, Avira AntiVir 7.11.1.163, Antiy Labs AVL SDK 2.0.3.7, avast! Antivirus 4.8.1351.0 and 5.0.677.0, AVG Anti-Virus 10.0.0.1190, Bitdefender 7.2, Quick Heal (aka Cat QuickHeal) 11.00, ClamAV 0.96.4, Command Antivirus 5.2.11.5, Comodo Antivirus 7424, Emsisoft Anti-Malware 5.1.0.1, F-Prot Antivirus 4.6.2.117, F-Secure Anti-Virus 9.0.16160.0, Fortinet Antivirus 4.2.254.0, G Data AntiVirus 21, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Jiangmin Antivirus 13.0.900, K7 AntiVirus 9.77.3565, Kaspersky Anti-Virus 7.0.0.125, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, Antimalware Engine 1.1.6402.0 in Microsoft Security Essentials 2.0, NOD32 Antivirus 5795, Norman Antivirus 6.06.12, nProtect Anti-Virus 2011-01-17.01, Panda Antivirus 10.0.2.7, PC Tools AntiVirus 7.0.3.5, Rising Antivirus 22.83.00.03, Sophos Anti-Virus 4.61.0, AVEngine 20101.3.0.103 in Symantec Endpoint Pr... |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2012-1461 | None | None | The Gzip file parser in AVG Anti-Virus 10.0.0.1190, Bitdefender 7.2, Command Antivirus 5.2.11.5, Emsisoft Anti-Malware 5.1.0.1, F-Secure Anti-Virus 9.0.16160.0, Fortinet Antivirus 4.2.254.0, Ikarus Virus Utilities T3 Command Line Scanner 1.1.97.0, Jiangmin Antivirus 13.0.900, K7 AntiVirus 9.77.3565, Kaspersky Anti-Virus 7.0.0.125, McAfee Anti-Virus Scanning Engine 5.400.0.1158, McAfee Gateway (formerly Webwasher) 2010.1C, NOD32 Antivirus 5795, Norman Antivirus 6.06.12, Rising Antivirus 22.83.00.03, Sophos Anti-Virus 4.61.0, AVEngine 20101.3.0.103 in Symantec Endpoint Protection 11, Trend Micro AntiVirus 9.120.0.1004, Trend Micro HouseCall 9.120.0.1004, and VBA32 3.12.14.2 allows remote attackers to bypass malware detection via a .tar.gz file with multiple compressed streams. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different Gzip parser implementations. |
| McAfee | 1.29.162.1 | CVE-2012-1463 | None | None | The ELF file parser in AhnLab V3 Internet Security 2011.01.18.00, Bitdefender 7.2, Quick Heal (aka Cat QuickHeal) 11.00, Command Antivirus 5.2.11.5, Comodo Antivirus 7424, eSafe 7.0.17.0, F-Prot Antivirus 4.6.2.117, F-Secure Anti-Virus 9.0.16160.0, McAfee Anti-Virus Scanning Engine 5.400.0.1158, Norman Antivirus 6.06.12, nProtect Anti-Virus 2011-01-17.01, and Panda Antivirus 10.0.2.7 allows remote attackers to bypass malware detection via an ELF file with a modified endianness field. NOTE: this may later be SPLIT into multiple CVEs if additional information is published showing that the error occurred independently in different ELF parser implementations.   |
| McAfee | 1.29.162.1 | CVE-2012-2212 | None | None | McAfee Web Gateway 7.0 allows remote attackers to bypass the access configuration for the CONNECT method by providing an arbitrary allowed hostname in the Host HTTP header. NOTE: this issue might not be reproducible, because the researcher did not provide configuration details for the vulnerable system, and the observed behavior might be consistent with a configuration that was (perhaps inadvertently) designed to allow access based on Host HTTP headers  |
| McAfee | 1.29.162.1 | CVE-2009-5115 | None | None | McAfee Common Management Agent (CMA) 3.5.5 through 3.5.5.588 and 3.6.0 through 3.6.0.608, and McAfee Agent 4.0 before Patch 3, allows remote authenticated users to overwrite arbitrary files by accessing a report-writing ActiveX control COM object.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2009-5116 | None | None | McAfee LinuxShield 1.5.1 and earlier does not properly implement client authentication, which allows remote authenticated users to obtain Admin access to the statistics server by leveraging a client account.   |
| McAfee | 1.29.162.1 | CVE-2009-5117 | None | None | The Web Post Protection feature in McAfee Host Data Loss Prevention (DLP) 3.x before 3.0.100.10 and 9.x before 9.0.0.422, when HTTP Capture mode is enabled, allows local users to obtain sensitive information from web traffic by reading unspecified files.  |
| McAfee | 1.29.162.1 | CVE-2009-5118 | None | None | Untrusted search path vulnerability in McAfee VirusScan Enterprise before 8.7i allows local users to gain privileges via a Trojan horse DLL in an unspecified directory, as demonstrated by scanning a document located on a remote share.  |
| McAfee | 1.29.162.1 | CVE-2010-3496 | None | None | McAfee VirusScan Enterprise 8.5i and 8.7i does not properly interact with the processing of hcp:// URLs by the Microsoft Help and Support Center, which makes it easier for remote attackers to execute arbitrary code via malware that is correctly detected by this product, but with a detection approach that occurs too late to stop the code execution. |
| McAfee | 1.29.162.1 | CVE-2010-5143 | None | None | McAfee VirusScan Enterprise before 8.8 allows local users to disable the product by leveraging administrative privileges to execute an unspecified Metasploit Framework module.   |
| McAfee | 1.29.162.1 | CVE-2011-5100 | None | None | The web interface in McAfee Firewall Reporter before 5.1.0.13 does not properly implement cookie authentication, which allows remote attackers to obtain access, and disable anti-virus functionality, via an HTTP request.   |
| McAfee | 1.29.162.1 | CVE-2011-5101 | None | None | The Rumor technology in McAfee SaaS Endpoint Protection before 5.2.4 allows remote attackers to relay e-mail messages via unspecified vectors, as demonstrated by relaying spam.  |
| McAfee | 1.29.162.1 | CVE-2012-4580 | None | None | Cross-site scripting (XSS) vulnerability in McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, allows remote attackers to inject arbitrary web script or HTML via vectors related to the McAfee Security Appliance Management Console/Dashboard.                           |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2012-4581 | None | None | McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, does not disable the server-side session token upon the closing of the Management Console/Dashboard, which makes it easier for remote attackers to hijack sessions by capturing a session cookie and then modifying the response to a login attempt, related to a "Logout Failure" issue. |
| McAfee | 1.29.162.1 | CVE-2012-4582 | None | None | McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, allows remote authenticated users to reset the passwords of arbitrary administrative accounts via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2012-4583 | None | None | McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, allows remote authenticated users to obtain the session tokens of arbitrary users by navigating within the Dashboard.   |
| McAfee | 1.29.162.1 | CVE-2012-4584 | None | None | McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, does not properly encrypt system-backup data, which makes it easier for remote authenticated users to obtain sensitive information by reading a backup file, as demonstrated by obtaining password hashes.  |
| McAfee | 1.29.162.1 | CVE-2012-4585 | None | None | McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, allows remote authenticated users to read arbitrary files via a crafted URL.  |
| McAfee | 1.29.162.1 | CVE-2012-4586 | None | None | McAfee Email and Web Security (EWS) 5.x before 5.5 Patch 6 and 5.6 before Patch 3, and McAfee Email Gateway (MEG) 7.0 before Patch 1, accesses files with the privileges of the root user, which allows remote authenticated users to bypass intended permission settings by requesting a file.   |
| McAfee | 1.29.162.1 | CVE-2012-4587 | None | None | McAfee Enterprise Mobility Manager (EMM) Agent before 4.8 and Server before 10.1, when one-time provisioning (OTP) mode is enabled, have an improper dependency on DNS SRV records, which makes it easier for remote attackers to discover user passwords by spoofing the EMM server, as demonstrated by a password entered on an iOS device.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2012-4588 | None | None | McAfee Enterprise Mobility Manager (EMM) Agent before 4.8 and Server before 10.1 record all invalid usernames presented in failed login attempts, and place them on a list of accounts that an administrator may wish to unlock, which allows remote attackers to cause a denial of service (excessive list size in the EMM Database) via a long sequence of login attempts with different usernames. |
| McAfee | 1.29.162.1 | CVE-2012-4589 | None | None | Login.aspx in the Portal in McAfee Enterprise Mobility Manager (EMM) before 10.0 does not have an off autocomplete attribute for unspecified form fields, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.  |
| McAfee | 1.29.162.1 | CVE-2012-4590 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in About.aspx in the Portal in McAfee Enterprise Mobility Manager (EMM) before 10.0 might allow remote attackers to inject arbitrary web script or HTML via the (1) User Agent or (2) Connection variable.  |
| McAfee | 1.29.162.1 | CVE-2012-4591 | None | None | About.aspx in the Portal in McAfee Enterprise Mobility Manager (EMM) before 10.0 discloses the name of the user account for an IIS worker process, which allows remote attackers to obtain potentially sensitive information by visiting this page.   |
| McAfee | 1.29.162.1 | CVE-2012-4592 | None | None | The Portal in McAfee Enterprise Mobility Manager (EMM) before 10.0 does not set the secure flag for the ASP.NET session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.  |
| McAfee | 1.29.162.1 | CVE-2012-4593 | None | None | McAfee Application Control and Change Control 5.1.x and 6.0.0 do not enforce an intended password requirement in certain situations involving attributes of the password file, which allows local users to bypass authentication by executing a command.  |
| McAfee | 1.29.162.1 | CVE-2012-4594 | None | None | McAfee ePolicy Orchestrator (ePO) 4.6.1 and earlier allows remote authenticated users to bypass intended access restrictions, and obtain sensitive information from arbitrary reporting panels, via a modified ID value in a console URL.   |
| McAfee | 1.29.162.1 | CVE-2012-4595 | None | None | McAfee Email and Web Security (EWS) 5.5 through Patch 6 and 5.6 through Patch 3, and McAfee Email Gateway (MEG) 7.0.0 and 7.0.1, allows remote attackers to bypass authentication and obtain an admin session ID via unspecified vectors.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2012-4596 | None | None | Directory traversal vulnerability in McAfee Email Gateway (MEG) 7.0.0 and 7.0.1 allows remote authenticated users to bypass intended access restrictions and download arbitrary files via a crafted URL.  |
| McAfee | 1.29.162.1 | CVE-2012-4597 | None | None | Cross-site scripting (XSS) vulnerability in McAfee Email and Web Security (EWS) 5.5 through Patch 6 and 5.6 through Patch 3, and McAfee Email Gateway (MEG) 7.0.0 and 7.0.1, allows remote attackers to inject arbitrary web script or HTML via vectors related to the McAfee Security Appliance Management Console/Dashboard.  |
| McAfee | 1.29.162.1 | CVE-2012-4598 | None | None | An unspecified ActiveX control in McAfee Virtual Technician (MVT) before 6.4, and ePO-MVT, allows remote attackers to execute arbitrary code or cause a denial of service (Internet Explorer crash) via a crafted web site.   |
| McAfee | 1.29.162.1 | CVE-2012-4599 | None | None | McAfee SmartFilter Administration, and SmartFilter Administration Bess Edition, before 4.2.1.01 does not require authentication for access to the JBoss Remote Method Invocation (RMI) interface, which allows remote attackers to execute arbitrary code via a crafted .war file.  |
| McAfee | 1.29.162.1 | CVE-2010-5166 | None | None | Race condition in McAfee Total Protection 2010 10.0.580 on Windows XP allows local users to bypass kernel-mode hook handlers, and execute dangerous code that would otherwise be blocked by a handler but not blocked by signature-based malware detection, via certain user-space memory changes during hook-handler execution, aka an argument-switch attack or a KHOBE attack. NOTE: this issue is disputed by some third parties because it is a flaw in a protection mechanism for situations where a crafted program has already begun to execute |
| McAfee | 1.29.162.1 | CVE-2012-4014 | None | None | Unspecified vulnerability in McAfee Email Anti-virus (formerly WebShield SMTP) allows remote attackers to cause a denial of service via unknown vectors.  |
| McAfee | 1.29.162.1 | CVE-2012-5879 | None | None | An ActiveX control in McHealthCheck.dll in McAfee Virtual Technician (MVT) and ePO-MVT 6.5.0.2101 and earlier allows remote attackers to modify or create arbitrary files via a full pathname argument to the Save method.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2013-0140 | None | None | SQL injection vulnerability in the Agent-Handler component in McAfee ePolicy Orchestrator (ePO) before 4.5.7 and 4.6.x before 4.6.6 allows remote attackers to execute arbitrary SQL commands via a crafted request over the Agent-Server communication channel.   |
| McAfee | 1.29.162.1 | CVE-2013-0141 | None | None | Directory traversal vulnerability in McAfee ePolicy Orchestrator (ePO) before 4.5.7 and 4.6.x before 4.6.6 allows remote attackers to upload arbitrary files via a crafted request over the Agent-Server communication channel, as demonstrated by writing to the Software/ directory.   |
| McAfee | 1.29.162.1 | CVE-2013-4882 | None | None | Multiple SQL injection vulnerabilities in McAfee ePolicy Orchestrator 4.6.6 and earlier, and the ePolicy Orchestrator (ePO) extension for McAfee Agent (MA) 4.5 and 4.6, allow remote authenticated users to execute arbitrary SQL commands via the uid parameter to (1) core/showRegisteredTypeDetails.do and (2) EPOAGENTMETA/DisplayMSAPropsDetails.do, a different vulnerability than CVE-2013-0140.   |
| McAfee | 1.29.162.1 | CVE-2013-4883 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in McAfee ePolicy Orchestrator 4.6.6 and earlier, and the ePO Extension for the McAfee Agent (MA) 4.5 through 4.6, allow remote attackers to inject arbitrary web script or HTML via the (1) instancelid parameter core/loadDisplayType.do; (2) instancelid or (3) monitorUrl parameter to console/createDashboardContainer.do; uid parameter to (4) ComputerMgmt/sysDetPanelBoolPicked.do or (5) ComputerMgmt/sysDetPanelSummary.do; (6) uid, (7) orion.user.security.token, or (8) ajaxMode parameter to ComputerMgmt/sysDetPanelQry.do; or (9) uid, (10) orion.user.security.token, or (11) ajaxMode parameter to ComputerMgmt/sysDetPanelSummary.do. |
| McAfee | 1.29.162.1 | CVE-2013-3627 | None | None | FrameworkService.exe in McAfee Framework Service in McAfee Managed Agent (MA) before 4.5.0.1927 and 4.6 before 4.6.0.3258 allows remote attackers to cause a denial of service (service crash) via a malformed HTTP request.   |
| McAfee | 1.29.162.1 | CVE-2013-6349 | None | None | McAfee Email Gateway (MEG) 7.0 before 7.0.4 and 7.5 before 7.5.1 allows remote authenticated users to execute arbitrary commands via unspecified vectors.  |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2013-7092 | None | None | Multiple SQL injection vulnerabilities in /admin/cgi-bin/rpc/doReport/18 in McAfee Email Gateway 7.6 allow remote authenticated users to execute arbitrary SQL commands via the (1) events_col, (2) event_id, (3) reason, (4) events_order, (5) emailstatus_order, or (6) emailstatus_col JSON keys.    |
| McAfee | 1.29.162.1 | CVE-2013-7103 | None | None | McAfee Email Gateway 7.6 allows remote authenticated administrators to execute arbitrary commands via shell metacharacters in the value attribute in a (1) TestFile XML element or the (2) hostname. NOTE: this issue can be combined with CVE-2013-7092 to allow remote attackers to execute commands. |
| McAfee | 1.29.162.1 | CVE-2013-7104 | None | None | McAfee Email Gateway 7.6 allows remote authenticated administrators to execute arbitrary commands by specifying them in the value attribute in a (1) Command or (2) Script XML element. NOTE: this issue can be combined with CVE-2013-7092 to allow remote attackers to execute commands.              |
| McAfee | 1.29.162.1 | CVE-2014-1472 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in the Enterprise Manager in McAfee Vulnerability Manager (MVM) 7.5.5 and earlier allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2014-1473 | None | None | Multiple cross-site request forgery (CSRF) vulnerabilities in the Enterprise Manager in McAfee Vulnerability Manager (MVM) 7.5.5 and earlier allow remote attackers to hijack the authentication of users for requests that modify HTML via unspecified vectors related to the "response web page."     |
| McAfee | 1.29.162.1 | CVE-2013-4884 | None | None | Cross-site scripting (XSS) vulnerability in McAfee SuperScan 4.0 allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded sequences in a server response, which is not properly handled in the SuperScan HTML report.   |
| McAfee | 1.29.162.1 | CVE-2013-5094 | None | None | Cross-site scripting (XSS) vulnerability in index.exp in McAfee Vulnerability Manager 7.5 allows remote attackers to inject arbitrary web script or HTML via the cert_cn cookie parameter.  |
| McAfee | 1.29.162.1 | CVE-2014-2205 | None | None | The Import and Export Framework in McAfee ePolicy Orchestrator (ePO) before 4.6.7 Hotfix 940148 allows remote authenticated users with permissions to add dashboards to read arbitrary files by importing a crafted XML file, related to an XML External Entity (XXE) issue.                            |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2014-2535 | None | None | Directory traversal vulnerability in McAfee Web Gateway (MWG) 7.4.x before 7.4.1, 7.3.x before 7.3.2.6, and 7.2.0.9 and earlier allows remote authenticated users to read arbitrary files via a crafted request to the web filtering port.   |
| McAfee | 1.29.162.1 | CVE-2014-2536 | None | None | Directory traversal vulnerability in McAfee Cloud Identity Manager 3.0, 3.1, and 3.5.1, McAfee Cloud Single Sign On (MCSSO) before 4.0.1, and Intel Expressway Cloud Access 360-SSO 2.1 and 2.5 allows remote authenticated users to read an unspecified file containing a hash of the administrator password via unknown vectors.   |
| McAfee | 1.29.162.1 | CVE-2014-2586 | None | None | Cross-site scripting (XSS) vulnerability in the login audit form in McAfee Cloud Single Sign On (SSO) allows remote attackers to inject arbitrary web script or HTML via a crafted password.   |
| McAfee | 1.29.162.1 | CVE-2014-2587 | None | None | SQL injection vulnerability in jsp/reports/ReportsAudit.jsp in McAfee Asset Manager 6.6 allows remote authenticated users to execute arbitrary SQL commands via the username of an audit report (aka user parameter).  |
| McAfee | 1.29.162.1 | CVE-2014-2588 | None | None | Directory traversal vulnerability in servlet/downloadReport in McAfee Asset Manager 6.6 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the reportFileName parameter.  |
| McAfee | 1.29.162.1 | CVE-2014-2390 | None | None | Cross-site request forgery (CSRF) vulnerability in the User Management module in McAfee Network Security Manager (NSM) before 6.1.15.39 7.1.5.x before 7.1.5.15, 7.1.15.x before 7.1.15.7, 7.5.x before 7.5.5.9, and 8.x before 8.1.7.3 allows remote attackers to hijack the authentication of users for requests that modify user accounts via unspecified vectors.                      |
| McAfee | 1.29.162.1 | CVE-2014-6064 | None | None | The Accounts tab in the administrative user interface in McAfee Web Gateway (MWG) before 7.3.2.9 and 7.4.x before 7.4.2 allows remote authenticated users to obtain the hashed user passwords via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2014-8518 | None | None | The (1) Removable Media and (2) CD and DVD encryption offsite access options (formerly Endpoint Encryption for Removable Media or EERM) in McAfee File and Removable Media Protection (FRP) 4.3.0.x, and Endpoint Encryption for Files and Folders (EEFF) 3.2.x through 4.2.x, uses a hard-coded salt, which makes it easier for local users to obtain passwords via a brute force attack. |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2014-8519 | None | None | Unspecified vulnerability in McAfee Network Data Loss Prevention (NDLP) before 9.2.2 allows local users to read arbitrary files via unknown vectors.   |
| McAfee | 1.29.162.1 | CVE-2014-8520 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 allows remote attackers to obtain sensitive information via vectors related to open network ports.   |
| McAfee | 1.29.162.1 | CVE-2014-8521 | None | None | Cross-site scripting (XSS) vulnerability in McAfee Network Data Loss Prevention (NDLP) before 9.3 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2014-8522 | None | None | The MySQL database in McAfee Network Data Loss Prevention (NDLP) before 9.3 does not require a password, which makes it easier for remote attackers to obtain access.  |
| McAfee | 1.29.162.1 | CVE-2014-8523 | None | None | Cross-site request forgery (CSRF) vulnerability in McAfee Network Data Loss Prevention (NDLP) before 9.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.  |
| McAfee | 1.29.162.1 | CVE-2014-8524 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 does not disable the autocomplete setting for the password and other fields, which allows remote attackers to obtain sensitive information via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2014-8525 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 does not include the HTTPOnly flag in a Set-Cookie header for the session cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie. |
| McAfee | 1.29.162.1 | CVE-2014-8526 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 allows local users to obtain sensitive information by reading a Java stack trace.  |
| McAfee | 1.29.162.1 | CVE-2014-8527 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 allows local users to obtain sensitive information and affect integrity via vectors related to a "plain text password."  |
| McAfee | 1.29.162.1 | CVE-2014-8528 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 logs session IDs, which allows local users to obtain sensitive information by reading the audit log.   |
| McAfee | 1.29.162.1 | CVE-2014-8529 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 stores the SSH key in cleartext, which allows local users to obtain sensitive information via unspecified vectors.   |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2014-8530 | None | None | Unspecified vulnerability in McAfee Network Data Loss Prevention (NDLP) before 9.3 allows remote attackers to obtain sensitive information, affect integrity, or cause a denial of service via unknown vectors, related to simultaneous logins.                                  |
| McAfee | 1.29.162.1 | CVE-2014-8531 | None | None | The TLS/SSL Server in McAfee Network Data Loss Prevention (NDLP) before 9.3 uses weak cipher algorithms, which makes it easier for remote authenticated users to execute arbitrary code via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2014-8532 | None | None | Unspecified vulnerability in McAfee Network Data Loss Prevention before (NDLP) before 9.3 allows local users to obtain sensitive information and impact integrity via unknown vectors, related to partition mounting.  |
| McAfee | 1.29.162.1 | CVE-2014-8533 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.3 allows remote attackers to execute arbitrary code via vectors related to ICMP redirection.   |
| McAfee | 1.29.162.1 | CVE-2014-8534 | None | None | Unspecified vulnerability in the login form in McAfee Network Data Loss Prevention (NDLP) before 9.2.2 allows local users to cause a denial of service via a crafted value in the domain field.  |
| McAfee | 1.29.162.1 | CVE-2014-8535 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.2.2 allows local users to bypass intended restriction on unspecified functionality via unknown vectors.  |
| McAfee | 1.29.162.1 | CVE-2014-8536 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.2.2 allows local users to obtain sensitive information by reading unspecified error messages.  |
| McAfee | 1.29.162.1 | CVE-2014-8537 | None | None | McAfee Network Data Loss Prevention (NDLP) before 9.2.2 allows local users to obtain sensitive information by reading the logs.  |
| McAfee | 1.29.162.1 | CVE-2015-0921 | None | None | XML external entity (XXE) vulnerability in the Server Task Log in McAfee ePolicy Orchestrator (ePO) before 4.6.9 and 5.x before 5.1.2 allows remote authenticated users to read arbitrary files via the conditionXML parameter to the taskLogTable to orionUpdateTableFilter.do. |
| McAfee | 1.29.162.1 | CVE-2015-0922 | None | None | McAfee ePolicy Orchestrator (ePO) before 4.6.9 and 5.x before 5.1.2 uses the same secret key across different customers' installations, which allows attackers to obtain the administrator password by leveraging knowledge of the encrypted password.                           |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2015-1305 | None | None | McAfee Data Loss Prevention Endpoint (DLPe) before 9.3.400 allows local users to write to arbitrary memory locations, and consequently gain privileges, via a crafted (1) 0x00224014 or (2) 0x0022c018 IOCTL call.  |
| McAfee | 1.29.162.1 | CVE-2015-1616 | None | None | SQL injection vulnerability in the ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3.400 allows remote authenticated ePO users to execute arbitrary SQL commands via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-1617 | None | None | Cross-site scripting (XSS) vulnerability in the ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3.400 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-1618 | None | None | The ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3.400 allows remote authenticated users to obtain sensitive password information via a crafted URL.   |
| McAfee | 1.29.162.1 | CVE-2015-1619 | None | None | Cross-site scripting (XSS) vulnerability in the Secure Web Mail Client user interface in McAfee Email Gateway (MEG) 7.6.x before 7.6.3.2, 7.5.x before 7.5.6, 7.0.x through 7.0.5, 5.6, and earlier allows remote authenticated users to inject arbitrary web script or HTML via unspecified tokens in Digest messages. |
| McAfee | 1.29.162.1 | CVE-2015-2053 | None | None | The log viewer in McAfee Agent (MA) before 4.8.0 Patch 3 and 5.0.0, when the "Accept connections only from the ePO server" option is disabled, allows remote attackers to conduct clickjacking attacks via a crafted web page, aka an "http-generic-click-jacking" vulnerability.                                       |
| McAfee | 1.29.162.1 | CVE-2015-2757 | None | None | The ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3 Patch 4 Hotfix 16 (9.3.416.4) allows remote authenticated users to cause a denial of service (database lock or license corruption) via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-2758 | None | None | The ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3 Patch 4 Hotfix 16 (9.3.416.4) allows remote authenticated users to obtain sensitive information, modify the database, or possibly have other unspecified impact via a crafted URL.  |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2015-2759 | None | None | Multiple cross-site request forgery (CSRF) vulnerabilities in the ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3 Patch 4 Hotfix 16 (9.3.416.4) allow remote attackers to hijack the authentication of users for requests that (1) obtain sensitive information or (2) modify the database via unspecified vectors. |
| McAfee | 1.29.162.1 | CVE-2015-2760 | None | None | Cross-site scripting (XSS) vulnerability in the ePO extension in McAfee Data Loss Prevention Endpoint (DLPe) before 9.3 Patch 4 Hotfix 16 (9.3.416.4) allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-3028 | None | None | McAfee Advanced Threat Defense (MATD) before 3.4.4.63 allows remote authenticated users to bypass intended restrictions and change or update configuration settings via crafted parameters.   |
| McAfee | 1.29.162.1 | CVE-2015-3029 | None | None | The web interface in McAfee Advanced Threat Defense (MATD) before 3.4.4.63 does not properly restrict access, which allows remote authenticated users to obtain sensitive information via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2015-3030 | None | None | The web interface in McAfee Advanced Threat Defense (MATD) before 3.4.4.63 allows remote authenticated users to obtain sensitive configuration information via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-3987 | None | None | Multiple unquoted Windows search path vulnerabilities in the (1) Client Management and (2) Gateway in McAfee ePO Deep Command 2.1 and 2.2 before HF 1058831 allow local users to gain privileges via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-4559 | None | None | Cross-site scripting (XSS) vulnerability in the product deployment feature in the Java core web services in Intel McAfee ePolicy Orchestrator (ePO) before 5.1.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2015-2859 | None | None | Intel McAfee ePolicy Orchestrator (ePO) 4.x through 4.6.9 and 5.x through 5.1.2 does not validate server names and Certification Authority names in X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.                              |
| McAfee | 1.29.162.1 | CVE-2015-7237 | None | None | Directory traversal vulnerability in the remote log viewing functionality in McAfee Agent (MA) 5.x before 5.0.2 allows remote attackers to obtain sensitive information via unspecified vectors.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2015-7310 | None | None | McAfee Enterprise Security Manager (ESM), Enterprise Security Manager/Log Manager (ESMLM), and Enterprise Security Manager/Receiver (ESMREC) before 9.3.2MR18, 9.4.x before 9.4.2MR8, and 9.5.x before 9.5.0MR7 allow remote authenticated users to execute arbitrary OS commands via a crafted filename, which is not properly handled when downloading the file.   |
| McAfee | 1.29.162.1 | CVE-2015-7612 | None | None | Multiple cross-site request forgery (CSRF) vulnerabilities in the Organizations page in Enterprise Manager in McAfee Vulnerability Manager (MVM) 7.5.9 and earlier allow remote attackers to hijack the authentication of administrators for requests that have unspecified impact via unknown vectors.  |
| McAfee | 1.29.162.1 | CVE-2015-8024 | None | None | McAfee Enterprise Security Manager (ESM), Enterprise Security Manager/Log Manager (ESMLM), and Enterprise Security Manager/Receiver (ESMREC) 9.3.x before 9.3.2MR19, 9.4.x before 9.4.2MR9, and 9.5.x before 9.5.0MR8, when configured to use Active Directory or LDAP authentication sources, allow remote attackers to bypass authentication by logging in with the username "NGCP NGCP NGCP;" and any password.           |
| McAfee | 1.29.162.1 | CVE-2015-8577 | None | None | The Buffer Overflow Protection (BOP) feature in McAfee VirusScan Enterprise before 8.8 Patch 6 allocates memory with Read, Write, Execute (RWX) permissions at predictable addresses on 32-bit platforms when protecting another application, which allows attackers to bypass the DEP and ASLR protection mechanisms via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2015-8765 | None | None | Intel McAfee ePolicy Orchestrator (ePO) 4.6.9 and earlier, 5.0.x, 5.1.x before 5.1.3 Hotfix 1106041, and 5.3.x before 5.3.1 Hotfix 1106041 allow remote attackers to execute arbitrary code via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.   |
| McAfee | 1.29.162.1 | CVE-2016-1715 | None | None | The swin.sys kernel driver in McAfee Application Control (MAC) 6.1.0 before build 706, 6.1.1 before build 404, 6.1.2 before build 449, 6.1.3 before build 441, and 6.2.0 before build 505 on 32-bit Windows platforms allows local users to cause a denial of service (memory corruption and system crash) or gain privileges via a 768 syscall, which triggers a zero to be written to an arbitrary kernel memory location. |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2015-8772 | None | None | McPvDrv.sys 4.6.111.0 in McAfee File Lock 5.x in McAfee Total Protection allows local users to obtain sensitive information from kernel memory or cause a denial of service (system crash) via a large VERIFY_INFORMATION.Length value in an IOCTL_DISK_VERIFY ioctl call.  |
| McAfee | 1.29.162.1 | CVE-2015-8773 | None | None | Stack-based buffer overflow in McPvDrv.sys 4.6.111.0 in McAfee File Lock 5.x in McAfee Total Protection allows attackers to cause a denial of service (system crash) via a long vault GUID in an ioctl call.  |
| McAfee | 1.29.162.1 | CVE-2016-2199 | None | None | Multiple cross-site request forgery (CSRF) vulnerabilities in the Organizations and Remediation management page in Enterprise Manager in McAfee Vulnerability Manager (MVM) before 7.5.10 allow remote attackers to hijack the authentication of administrators for requests that have unspecified impact via unknown vectors.  |
| McAfee | 1.29.162.1 | CVE-2016-3969 | None | None | Cross-site scripting (XSS) vulnerability in McAfee Email Gateway (MEG) 7.6.x before 7.6.404, when File Filtering is enabled with the action set to ESERVICES:REPLACE, allows remote attackers to inject arbitrary web script or HTML via an attachment in a blocked email.  |
| McAfee | 1.29.162.1 | CVE-2016-3983 | None | None | McAfee Advanced Threat Defense (ATD) before 3.4.8.178 might allow remote attackers to bypass malware detection by leveraging information about the parent process.  |
| McAfee | 1.29.162.1 | CVE-2016-3984 | None | None | The McAfee VirusScan Console (mcconsol.exe) in McAfee Active Response (MAR) before 1.1.0.161, Agent (MA) 5.x before 5.0.2 Hotfix 1110392 (5.0.2.333), Data Exchange Layer 2.x (DXL) before 2.0.1.140.1, Data Loss Prevention Endpoint (DLPe) 9.3 before Patch 6 and 9.4 before Patch 1 HF3, Device Control (MDC) 9.3 before Patch 6 and 9.4 before Patch 1 HF3, Endpoint Security (ENS) 10.x before 10.1, Host Intrusion Prevention Service (IPS) 8.0 before 8.0.0.3624, and VirusScan Enterprise (VSE) 8.8 before P7 (8.8.0.1528) on Windows allows local administrators to bypass intended self-protection rules and disable the antivirus engine by modifying registry keys. |
| McAfee | 1.29.162.1 | CVE-2016-4534 | None | None | The McAfee VirusScan Console (mcconsol.exe) in McAfee VirusScan Enterprise 8.8.0 before Hotfix 1123565 (8.8.0.1546) on Windows allows local administrators to bypass intended self-protection rules and unlock the console window by closing registry handles.  |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2016-4535 | None | None | Integer signedness error in the AV engine before DAT 8145, as used in McAfee LiveSafe 14.0, allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted packed executable.   |
| McAfee | 1.29.162.1 | CVE-2016-8006 | None | None | Authentication bypass vulnerability in Enterprise Security Manager (ESM) and License Manager (LM) in Intel Security McAfee Security Information and Event Management (SIEM) 9.6.0 MR3 allows an administrator to make changes to other SIEM users' information including user passwords without supplying the current administrator password a second time via the GUI or GUI terminal commands.  |
| McAfee | 1.29.162.1 | CVE-2017-3896 | None | None | Unvalidated parameter vulnerability in the remote log viewing capability in Intel Security McAfee Agent 5.0.x versions prior to 5.0.4.449 allows remote attackers to pass unexpected input parameters via a URL that was not completely validated.  |
| McAfee | 1.29.162.1 | CVE-2013-7460 | None | None | A write protection and execution bypass vulnerability in McAfee (now Intel Security) Application Control (MAC) 6.1.0 for Linux and earlier allows authenticated users to change binaries that are part of the Application Control whitelist and allows execution of binaries via specific conditions.   |
| McAfee | 1.29.162.1 | CVE-2013-7461 | None | None | A write protection and execution bypass vulnerability in McAfee (now Intel Security) Change Control (MCC) 6.1.0 for Linux and earlier allows authenticated users to change files that are part of write protection rules via specific conditions.   |
| McAfee | 1.29.162.1 | CVE-2013-7462 | None | None | A directory traversal vulnerability in the web application in McAfee (now Intel Security) SaaS Control Console (SCC) Platform 6.14 before patch 1070, and 6.15 before patch 1076 allows unauthenticated users to view contents of arbitrary system files that did not have file system level read access restrictions via a null-byte injection exploit.  |
| McAfee | 1.29.162.1 | CVE-2014-9920 | None | None | Unauthorized execution of binary vulnerability in McAfee (now Intel Security) McAfee Application Control (MAC) 6.0.0 before hotfix 9726, 6.0.1 before hotfix 9068, 6.1.0 before hotfix 692, 6.1.1 before hotfix 399, 6.1.2 before hotfix 426, and 6.1.3 before hotfix 357 and earlier allows attackers to create a malformed Windows binary that is considered non-executable and is not protected through the whitelisting protection feature via a specific set of circumstances. |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2014-9921 | None | None | Information disclosure vulnerability in McAfee (now Intel Security) Cloud Analysis and Deconstructive Services (CADS) 1.0.0.3x, 1.0.0.4d and earlier allows remote unauthenticated users to view, add, and remove users via a configuration error.   |
| McAfee | 1.29.162.1 | CVE-2015-8986 | None | None | Sandbox detection evasion vulnerability in hardware appliances in McAfee (now Intel Security) Advanced Threat Defense (MATD) 3.4.2.32 and earlier allows attackers to detect the sandbox environment, then bypass proper malware detection resulting in failure to detect a malware file (false-negative) via specially crafted malware. |
| McAfee | 1.29.162.1 | CVE-2015-8987 | None | None | Man-in-the-middle (MitM) attack vulnerability in non-Mac OS agents in McAfee (now Intel Security) Agent (MA) 4.8.0 patch 2 and earlier allows attackers to make a McAfee Agent talk with another, possibly rogue, ePO server via McAfee Agent migration to another ePO server.   |
| McAfee | 1.29.162.1 | CVE-2015-8988 | None | None | Unquoted executable path vulnerability in Client Management and Gateway components in McAfee (now Intel Security) ePO Deep Command (eDC) 2.2 and 2.1 allows authenticated users to execute a command of their choice via dropping a malicious file for the path.   |
| McAfee | 1.29.162.1 | CVE-2015-8989 | None | None | Unsalted password vulnerability in the Enterprise Manager (web portal) component in Intel Security McAfee Vulnerability Manager (MVM) 7.5.8 and earlier allows attackers to more easily decrypt user passwords via brute force attacks against the database.   |
| McAfee | 1.29.162.1 | CVE-2015-8991 | None | None | Malicious file execution vulnerability in Intel Security McAfee Security Scan+ (MSS+) before 3.11.266.3 allows attackers to make the product momentarily vulnerable via executing preexisting specifically crafted malware during installation or uninstallation, but not during normal operation.                                       |
| McAfee | 1.29.162.1 | CVE-2016-8005 | None | None | File extension filtering vulnerability in Intel Security McAfee Email Gateway (MEG) before 7.6.404h1128596 allows attackers to fail to identify the file name properly via scanning an email with a forged attached filename that uses a null byte within the filename extension.  |
| McAfee | 1.29.162.1 | CVE-2016-8007 | None | None | Authentication bypass vulnerability in McAfee Host Intrusion Prevention Services (HIPS) 8.0 Patch 7 and earlier allows authenticated users to manipulate the product's registry keys via specific conditions.  |

|        |            |               |      |      |  |
|--------|------------|---------------|------|------|--|
| McAfee | 1.29.162.1 | CVE-2016-8008 | None | None | Privilege escalation vulnerability in Windows 7 and Windows 10 in McAfee Security Scan Plus (SSP) 3.11.376 allows attackers to load a replacement of the version.dll file via McAfee McUICnt.exe onto a Windows system.  |
| McAfee | 1.29.162.1 | CVE-2016-8009 | None | None | Privilege escalation vulnerability in Intel Security McAfee Application Control (MAC) 7.0 and 6.x versions allows attackers to cause DoS, unexpected behavior, or potentially unauthorized code execution via an unauthorized use of IOCTL call.   |
| McAfee | 1.29.162.1 | CVE-2016-8010 | None | None | Application protections bypass vulnerability in Intel Security McAfee Application Control (MAC) 7.0 and earlier and Endpoint Security (ENS) 10.2 and earlier allows local users to bypass local security protection via a command-line utility.  |
| McAfee | 1.29.162.1 | CVE-2016-8011 | None | None | Cross-site scripting vulnerability in Intel Security McAfee Endpoint Security (ENS) Web Control before 10.2.0.408.10 allows attackers to inject arbitrary web script or HTML via a crafted web site.   |
| McAfee | 1.29.162.1 | CVE-2016-8026 | None | None | Arbitrary command execution vulnerability in Intel Security McAfee Security Scan Plus (SSP) 3.11.469 and earlier allows authenticated users to gain elevated privileges via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2016-8027 | None | None | SQL injection vulnerability in core services in Intel Security McAfee ePolicy Orchestrator (ePO) 5.3.2 and earlier and 5.1.3 and earlier allows attackers to alter a SQL query, which can result in disclosure of information within the database or impersonation of an agent without authentication via a specially crafted HTTP post. |
| McAfee | 1.29.162.1 | CVE-2016-8030 | None | None | A memory corruption vulnerability in Scriptscan COM Object in McAfee VirusScan Enterprise 8.8 Patch 8 and earlier allows remote attackers to create a Denial of Service on the active Internet Explorer tab via a crafted HTML link.   |
| McAfee | 1.29.162.1 | CVE-2017-4011 | None | None | Embedding Script (XSS) in HTTP Headers vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to get session/cookie information via modification of the HTTP request.   |
| McAfee | 1.29.162.1 | CVE-2017-4012 | None | None | Privilege Escalation vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to view confidential information via modification of the HTTP request.  |

|        |            |               |        |      |   |
|--------|------------|---------------|--------|------|---|
| McAfee | 1.29.162.1 | CVE-2017-4013 | None   | None | Banner Disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to obtain product information via HTTP response header.   |
| McAfee | 1.29.162.1 | CVE-2017-4014 | None   | None | Session Side jacking vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to view, add, and remove users via modification of the HTTP request.   |
| McAfee | 1.29.162.1 | CVE-2017-4015 | MEDIUM | 4.5  | Clickjacking vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to inject arbitrary web script or HTML via HTTP response header.   |
| McAfee | 1.29.162.1 | CVE-2017-4016 | None   | None | Web Server method disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to exploit and find another hole via HTTP response header.   |
| McAfee | 1.29.162.1 | CVE-2017-4017 | None   | None | User Name Disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to view user information via the appliance web interface.  |
| McAfee | 1.29.162.1 | CVE-2017-3980 | None   | None | A directory traversal vulnerability in the ePO Extension in McAfee ePolicy Orchestrator (ePO) 5.9.0, 5.3.2, and 5.1.3 and earlier allows remote authenticated users to execute a command of their choice via an authenticated ePO session.  |
| McAfee | 1.29.162.1 | CVE-2017-3948 | None   | None | Cross Site Scripting (XSS) in IMG Tags in the ePO extension in McAfee Data Loss Prevention Endpoint (DLP Endpoint) 10.0.x allows authenticated users to inject arbitrary web script or HTML via injecting malicious JavaScript into a user's browsing session.  |
| McAfee | 1.29.162.1 | CVE-2017-4052 | None   | None | Authentication Bypass vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote unauthenticated users / remote attackers to change or update any configuration settings, or gain administrator functionality via a crafted HTTP request parameter. |
| McAfee | 1.29.162.1 | CVE-2017-4053 | None   | None | Command Injection vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote unauthenticated users / remote attackers to execute a command of their choice via a crafted HTTP request parameter.  |
| McAfee | 1.29.162.1 | CVE-2017-4054 | None   | None | Command Injection vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote authenticated users to execute a command of their choice via a crafted HTTP request parameter.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2017-4055 | None | None | Exploitation of Authentication vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote unauthenticated users / remote attackers to bypass ATD detection via loose enforcement of authentication and authorization.                         |
| McAfee | 1.29.162.1 | CVE-2017-4057 | None | None | Privilege Escalation vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote authenticated users to gain elevated privileges via the GUI or GUI terminal commands.   |
| McAfee | 1.29.162.1 | CVE-2017-3897 | None | None | A Code Injection vulnerability in the non-certificate-based authentication mechanism in McAfee Live Safe versions prior to 16.0.3 and McAfee Security Scan Plus (MSS+) versions prior to 3.11.599.3 allows network attackers to perform a malicious file execution via a HTTP backend-response. |
| McAfee | 1.29.162.1 | CVE-2017-3898 | None | None | A man-in-the-middle attack vulnerability in the non-certificate-based authentication mechanism in McAfee LiveSafe (MLS) versions prior to 16.0.3 allows network attackers to modify the Windows registry value associated with the McAfee update via the HTTP backend-response.                 |
| McAfee | 1.29.162.1 | CVE-2017-3933 | None | None | Embedding Script (XSS) in HTTP Headers vulnerability in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to view confidential information via a cross site request forgery attack.  |
| McAfee | 1.29.162.1 | CVE-2017-3934 | None | None | Missing HTTP Strict Transport Security state information vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows man-in-the-middle attackers to expose confidential data via read files on the webserver.  |
| McAfee | 1.29.162.1 | CVE-2018-6660 | None | None | Directory Traversal vulnerability in McAfee ePolicy Orchestrator (ePO) 5.3.2, 5.3.1, 5.3.0 and 5.9.0 allows administrators to use Windows alternate data streams, which could be used to bypass the file extensions, via not properly validating the path when exporting a particular XML file. |
| McAfee | 1.29.162.1 | CVE-2018-6661 | HIGH | 7.8  | DLL Side-Loading vulnerability in Microsoft Windows Client in McAfee True Key before 4.20.110 allows local users to gain privilege elevation via not verifying a particular DLL file signature.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2018-6659 | None | None | Reflected Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) 5.3.2, 5.3.1, 5.3.0 and 5.9.0 allows remote authenticated users to exploit an XSS issue via not sanitizing the user input.  |
| McAfee | 1.29.162.1 | CVE-2017-3972 | None | None | Infrastructure-based foot printing vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows attackers to execute arbitrary code via the server banner leaking potentially sensitive or security relevant information.  |
| McAfee | 1.29.162.1 | CVE-2017-4028 | None | None | Maliciously misconfigured registry vulnerability in all Microsoft Windows products in McAfee consumer and corporate products allows an administrator to inject arbitrary code into a debugged McAfee process via manipulation of registry parameters.   |
| McAfee | 1.29.162.1 | CVE-2017-3964 | None | None | Reflective Cross-Site Scripting (XSS) vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows attackers to inject arbitrary web script or HTML via a URL parameter.   |
| McAfee | 1.29.162.1 | CVE-2017-3965 | None | None | Cross-Site Request Forgery (CSRF) (aka Session Riding) vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows remote attackers to perform unauthorized tasks such as retrieving internal system information or manipulating the database via specially crafted URLs. |
| McAfee | 1.29.162.1 | CVE-2017-3966 | None | None | Exploitation of session variables, resource IDs and other trusted credentials vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows remote attackers to exploit or harm a user's browser via reusing the exposed session token in the application URL.              |
| McAfee | 1.29.162.1 | CVE-2017-3967 | None | None | Target influence via framing vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows remote attackers to inject arbitrary web script or HTML via application pages inability to break out of 3rd party HTML frames.   |
| McAfee | 1.29.162.1 | CVE-2017-3969 | None | None | Abuse of communication channels vulnerability in the server in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows man-in-the-middle attackers to decrypt messages via an inadequate implementation of SSL.   |

|        |            |               |      |      |   |
|--------|------------|---------------|------|------|---|
| McAfee | 1.29.162.1 | CVE-2017-3971 | None | None | Cryptanalysis vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows attackers to view confidential information via insecure use of RC4 encryption cyphers.  |
| McAfee | 1.29.162.1 | CVE-2017-3961 | None | None | Cross-Site Scripting (XSS) vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows authenticated users to allow arbitrary HTML code to be reflected in the response web page via crafted user input of attributes.  |
| McAfee | 1.29.162.1 | CVE-2018-6664 | None | None | Application Protections Bypass vulnerability in Microsoft Windows in McAfee Data Loss Prevention (DLP) Endpoint before 10.0.500 and DLP Endpoint before 11.0.400 allows authenticated users to bypass the product block action via a command-line utility.  |
| McAfee | 1.29.162.1 | CVE-2018-6674 | None | None | Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 13 allows local users to spawn unrelated processes with elevated privileges via the system administrator granting McTray.exe elevated privileges (by default it runs with the current user's privileges). |
| McAfee | 1.29.162.1 | CVE-2018-6662 | HIGH | 7.8  | Privilege Escalation vulnerability in McAfee Management of Native Encryption (MNE) before 4.1.4 allows local users to gain elevated privileges via a crafted user input.  |
| McAfee | 1.29.162.1 | CVE-2018-6670 | None | None | External Entity Attack vulnerability in the ePO extension in McAfee Common UI (CUI) 2.0.2 allows remote authenticated users to view confidential information via a crafted HTTP request parameter.  |
| McAfee | 1.29.162.1 | CVE-2017-3960 | None | None | Exploitation of Authorization vulnerability in the web interface in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows authenticated users to gain elevated privileges via a crafted HTTP request parameter.   |
| McAfee | 1.29.162.1 | CVE-2017-3962 | None | None | Password recovery exploitation vulnerability in the non-certificate-based authentication mechanism in McAfee Network Security Management (NSM) before 8.2.7.42.2 allows attackers to crack user passwords via unsalted hashes.  |

|        |            |               |          |      |  |
|--------|------------|---------------|----------|------|--|
| McAfee | 1.29.162.1 | CVE-2017-3968 | None     | None | Session fixation vulnerability in the web interface in McAfee Network Security Manager (NSM) before 8.2.7.42.2 and McAfee Network Data Loss Prevention (NDLP) before 9.3.4.1.5 allows remote attackers to disclose sensitive information or manipulate the database via a crafted authentication cookie. |
| McAfee | 1.29.162.1 | CVE-2017-3907 | None     | None | Code Injection vulnerability in the ePolicy Orchestrator (ePO) extension in McAfee Threat Intelligence Exchange (TIE) Server 2.1.0 and earlier allows remote attackers to execute arbitrary HTML code to be reflected in the response web page via unspecified vector.                                   |
| McAfee | 1.29.162.1 | CVE-2017-3936 | None     | None | OS Command Injection vulnerability in McAfee ePolicy Orchestrator (ePO) 5.9.0, 5.3.2, 5.3.1, 5.1.3, 5.1.2, 5.1.1, and 5.1.0 allows attackers to run arbitrary OS commands with limited privileges via not sanitizing the user input data before exporting it into a CSV format output.                   |
| McAfee | 1.29.162.1 | CVE-2018-6671 | None     | None | Application Protection Bypass vulnerability in McAfee ePolicy Orchestrator (ePO) 5.3.0 through 5.3.3 and 5.9.0 through 5.9.1 allows remote authenticated users to bypass localhost only access security protection for some ePO features via a specially crafted HTTP request.                           |
| McAfee | 1.29.162.1 | CVE-2018-6672 | None     | None | Information disclosure vulnerability in McAfee ePolicy Orchestrator (ePO) 5.3.0 through 5.3.3 and 5.9.0 through 5.9.1 allows authenticated users to view sensitive information in plain text format via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2018-6667 | None     | None | Authentication Bypass vulnerability in the administrative user interface in McAfee Web Gateway 7.8.1.0 through 7.8.1.5 allows remote attackers to execute arbitrary code via Java management extensions (JMX).   |
| McAfee | 1.29.162.1 | CVE-2018-6681 | MEDIUM   | 5.4  | Abuse of Functionality vulnerability in the web interface in McAfee Network Security Management (NSM) 9.1.7.11 and earlier allows authenticated users to allow arbitrary HTML code to be reflected in the response web page via appliance web interface.   |
| McAfee | 1.29.162.1 | CVE-2018-6677 | CRITICAL | 9.1  | Directory Traversal vulnerability in the administrative user interface in McAfee Web Gateway (MWG) MWG 7.8.1.x allows authenticated administrator users to gain elevated privileges via unspecified vectors.   |

|        |            |               |          |      |   |
|--------|------------|---------------|----------|------|---|
| McAfee | 1.29.162.1 | CVE-2018-6678 | CRITICAL | 9.1  | Configuration/Environment manipulation vulnerability in the administrative interface in McAfee Web Gateway (MWG) MWG 7.8.1.x allows authenticated administrator users to execute arbitrary commands via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2018-6683 | HIGH     | 7.4  | Exploiting Incorrectly Configured Access Control Security Levels vulnerability in McAfee Data Loss Prevention (DLP) for Windows versions prior to 10.0.505 and 11.0.405 allows local users to bypass DLP policy via editing of local policy files when offline.       |
| McAfee | 1.29.162.1 | CVE-2018-6686 | MEDIUM   | 6.6  | Authentication Bypass vulnerability in TPM autoboot in McAfee Drive Encryption (MDE) 7.1.0 and above allows physically proximate attackers to bypass local security protection via specific set of circumstances.   |
| McAfee | 1.29.162.1 | CVE-2017-3912 | None     | None | Bypassing password security vulnerability in McAfee Application and Change Control (MACC) 7.0.1 and 6.2.0 allows authenticated users to perform arbitrary command execution via a command-line utility.   |
| McAfee | 1.29.162.1 | CVE-2018-6690 | HIGH     | 7.1  | Accessing, modifying, or executing executable files vulnerability in Microsoft Windows client in McAfee Application and Change Control (MACC) 8.0.0 Hotfix 4 and earlier allows authenticated users to execute arbitrary code via file transfer from external system. |
| McAfee | 1.29.162.1 | CVE-2018-6682 | MEDIUM   | 6.1  | Cross Site Scripting Exposure in McAfee True Key (TK) 4.0.0.0 and earlier allows local users to expose confidential data via a crafted web site.  |
| McAfee | 1.29.162.1 | CVE-2018-6700 | HIGH     | 7.8  | DLL Search Order Hijacking vulnerability in Microsoft Windows Client in McAfee True Key (TK) before 5.1.165 allows local users to execute arbitrary code via specially crafted malware.   |
| McAfee | 1.29.162.1 | CVE-2018-6689 | HIGH     | 7.8  | Authentication Bypass vulnerability in McAfee Data Loss Prevention Endpoint (DLPe) 10.0.x earlier than 10.0.510, and 11.0.x earlier than 11.0.600 allows attackers to bypass local security protection via specific conditions.                                       |
| McAfee | 1.29.162.1 | CVE-2018-6695 | MEDIUM   | 5.9  | SSH host keys generation vulnerability in the server in McAfee Threat Intelligence Exchange Server (TIE Server) 1.3.0, 2.0.x, 2.1.x, 2.2.0 allows man-in-the-middle attackers to spoof servers via acquiring keys from another environment.                           |
| McAfee | 1.29.162.1 | CVE-2018-6755 | None     | None | Weak Directory Permission Vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute arbitrary code via specially crafted malware.   |

|        |            |               |          |      |  |
|--------|------------|---------------|----------|------|--|
| McAfee | 1.29.162.1 | CVE-2018-6756 | None     | None | Authentication Abuse vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute unauthorized commands via specially crafted malware.  |
| McAfee | 1.29.162.1 | CVE-2018-6757 | None     | None | Privilege Escalation vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute arbitrary code via specially crafted malware.   |
| McAfee | 1.29.162.1 | CVE-2018-6703 | CRITICAL | 9.8  | Use After Free in Remote logging (which is disabled by default) in McAfee McAfee Agent (MA) 5.x prior to 5.6.0 allows remote unauthenticated attackers to cause a Denial of Service and potentially a remote code execution via a specially crafted HTTP header sent to the logging service.   |
| McAfee | 1.29.162.1 | CVE-2018-6704 | HIGH     | 7.8  | Privilege escalation vulnerability in McAfee Agent (MA) for Linux 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to perform arbitrary command execution via specific conditions.   |
| McAfee | 1.29.162.1 | CVE-2018-6705 | HIGH     | 7.8  | Privilege escalation vulnerability in McAfee Agent (MA) for Linux 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to perform arbitrary command execution via specific conditions.   |
| McAfee | 1.29.162.1 | CVE-2018-6706 | HIGH     | 7.5  | Insecure handling of temporary files in non-Windows McAfee Agent 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows an Unprivileged User to introduce custom paths during agent installation in Linux via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2018-6707 | None     | None | Denial of Service through Resource Depletion vulnerability in the agent in non-Windows McAfee Agent (MA) 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to cause DoS, unexpected behavior, or potentially unauthorized code execution via knowledge of the internal trust mechanism. |
| McAfee | 1.29.162.1 | CVE-2018-6669 | None     | None | A whitelist bypass vulnerability in McAfee Application Control / Change Control 7.0.1 and before allows a remote or local user to execute blacklisted files through an ASP.NET form.   |
| McAfee | 1.29.162.1 | CVE-2018-6668 | None     | None | A whitelist bypass vulnerability in McAfee Application Control / Change Control 7.0.1 and before allows execution bypass, for example, with simple DLL through interpreters such as PowerShell.  |
| McAfee | 1.29.162.1 | CVE-2019-3581 | None     | None | Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.  |

|        |            |               |        |      |  |
|--------|------------|---------------|--------|------|--|
| McAfee | 1.29.162.1 | CVE-2019-3584 | None   | None | Exploitation of Authentication vulnerability in MVision Endpoint in McAfee MVision Endpoint Prior to 1811 Update 1 (18.11.31.62) allows authenticated administrator users --> administrators to Remove MVision Endpoint via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2019-3587 | None   | None | DLL Search Order Hijacking vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Prior to 16.0.18 allows local users to execute arbitrary code via execution from a compromised folder.   |
| McAfee | 1.29.162.1 | CVE-2019-3593 | None   | None | Exploitation of Privilege/Trust vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Prior to 16.0.R18 allows local users to bypass product self-protection, tamper with policies and product files, and uninstall McAfee software without permission via specially crafted malware. |
| McAfee | 1.29.162.1 | CVE-2019-3604 | None   | None | Cross-Site Request Forgery (CSRF) vulnerability in McAfee ePO (legacy) Cloud allows unauthenticated users to perform unintended ePO actions using an authenticated user's session via unspecified vectors.   |
| McAfee | 1.29.162.1 | CVE-2019-3610 | None   | None | Data Leakage Attacks vulnerability in Microsoft Windows client in McAfee True Key (TK) 3.1.9211.0 and earlier allows local users to expose confidential data via specially crafted malware.  |
| McAfee | 1.29.162.1 | CVE-2018-6687 | MEDIUM | 5.5  | Loop with Unreachable Exit Condition ('Infinite Loop') in McAfee GetSusp (GetSusp) 3.0.0.461 and earlier allows attackers to DoS a manual GetSusp scan via while scanning a specifically crafted file . GetSusp is a free standalone McAfee tool that runs on several versions of Microsoft Windows.       |
| McAfee | 1.29.162.1 | CVE-2019-3582 | None   | None | Privilege Escalation vulnerability in Microsoft Windows client in McAfee Endpoint Security (ENS) 10.6.1 and earlier allows local users to gain elevated privileges via a specific set of circumstances.  |
| McAfee | 1.29.162.1 | CVE-2019-3598 | None   | None | Buffer Access with Incorrect Length Value in McAfee Agent (MA) 5.x allows remote unauthenticated users to potentially cause a denial of service via specifically crafted UDP packets.  |
| McAfee | 1.29.162.1 | CVE-2019-3599 | HIGH   | 7.5  | Information Disclosure vulnerability in Remote logging (which is disabled by default) in McAfee Agent (MA) 5.x allows remote unauthenticated users to access sensitive information via remote logging when it is enabled.  |

|        |            |               |        |      |   |
|--------|------------|---------------|--------|------|---|
| McAfee | 1.29.162.1 | CVE-2019-3615 | None   | None | Data Leakage Attacks vulnerability in the web interface in McAfee Database Security prior to the 4.6.6 March 2019 update allows local users to expose passwords via incorrectly auto completing password fields in the admin browser login screen.  |
| McAfee | 1.29.162.1 | CVE-2019-3597 | None   | None | Authentication Bypass vulnerability in McAfee Network Security Manager (NSM) 9.1 < 9.1.7.75.2 and 9.2 < 9.2.7.31 (9.2 Update 2) allows unauthenticated users to gain administrator rights via incorrect handling of expired GUI sessions.   |
| McAfee | 1.29.162.1 | CVE-2019-3606 | None   | None | Data Leakage Attacks vulnerability in the web portal component when in an MDR pair in McAfee Network Security Management (NSM) 9.1 < 9.1.7.75 (Update 4) and 9.2 < 9.2.7.31 Update2 allows administrators to view configuration information in plain text format via the GUI or GUI terminal commands.  |
| McAfee | 1.29.162.1 | CVE-2019-3612 | MEDIUM | 4.4  | Information Disclosure vulnerability in McAfee DXL Platform and TIE Server in DXL prior to 5.0.1 HF2 and TIE prior to 2.3.1 HF1 allows Authenticated users to view sensitive information in plain text via the GUI or command line.   |
| McAfee | 1.29.162.1 | CVE-2019-3586 | HIGH   | 7.5  | Protection Mechanism Failure in the Firewall in McAfee Endpoint Security (ENS) 10.x prior to 10.6.1 May 2019 update allows context-dependent attackers to circumvent ENS protection where GTI flagged IP addresses are not blocked by the ENS Firewall via specially crafted malicious sites where the GTI reputation is carefully manipulated and does not correctly trigger the ENS Firewall to block the connection. |
| McAfee | 1.29.162.1 | CVE-2019-3602 | None   | None | Cross Site Scripting (XSS) vulnerability in McAfee Network Security Manager (NSM) Prior to 9.1 Update 5 allows an authenticated administrator to embed an XSS in the administrator interface via a specially crafted custom rule containing HTML.   |
| McAfee | 1.29.162.1 | CVE-2019-3628 | HIGH   | 8.8  | Privilege escalation in McAfee Enterprise Security Manager (ESM) 11.x prior to 11.2.0 allows authenticated user to gain access to a core system component via incorrect access control.   |
| McAfee | 1.29.162.1 | CVE-2019-3629 | MEDIUM | 6.5  | Application protection bypass vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows unauthenticated user to impersonate system users via specially crafted parameters.   |

|        |            |               |        |      |   |
|--------|------------|---------------|--------|------|---|
| McAfee | 1.29.162.1 | CVE-2019-3630 | HIGH   | 7.2  | Command Injection vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows authenticated user to execute arbitrary code via specially crafted parameters.   |
| McAfee | 1.29.162.1 | CVE-2019-3631 | HIGH   | 7.2  | Command Injection vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows authenticated user to execute arbitrary code via specially crafted parameters.   |
| McAfee | 1.29.162.1 | CVE-2019-3632 | HIGH   | 8.8  | Directory Traversal vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows authenticated user to gain elevated privileges via specially crafted input.  |
| McAfee | 1.29.162.1 | CVE-2019-3619 | None   | None | Information Disclosure vulnerability in the Agent Handler in McAfee ePolicy Orchestrator (ePO) 5.9.x and 5.10.0 prior to 5.10.0 update 4 allows remote unauthenticated attacker to view sensitive information in plain text via sniffing the traffic between the Agent Handler and the SQL server.  |
| McAfee | 1.29.162.1 | CVE-2019-3592 | None   | None | Privilege escalation vulnerability in McAfee Agent (MA) before 5.6.1 HF3, allows local administrator users to potentially disable some McAfee processes by manipulating the MA directory control and placing a carefully constructed file in the MA directory.  |
| McAfee | 1.29.162.1 | CVE-2019-3591 | None   | None | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in ePO extension in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.0 allows unauthenticated remote user to trigger specially crafted JavaScript to render in the ePO UI via a carefully crafted upload to a remote website which is correctly blocked by DLPe Web Protection. This would then render as an XSS when the DLP Admin viewed the event in the ePO UI. |
| McAfee | 1.29.162.1 | CVE-2019-3595 | MEDIUM | 6.5  | Improper Neutralization of Special Elements used in a Command ('Command Injection') in ePO extension in McAfee Data Loss Prevention (DLP) 11.x prior to 11.3.0 allows Authenticated Administrator to execute arbitrary code with their local machine privileges via a specially crafted DLP policy, which is exported and opened on the their machine. In our checks, the user must explicitly allow the code to execute.   |

|        |            |               |                    |            |  |
|--------|------------|---------------|--------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2019-3622 | HIGH               | 8.2        | Files or Directories Accessible to External Parties in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.0 allows authenticated user to redirect DLPe log files to arbitrary locations via incorrect access control applied to the DLPe log folder allowing privileged users to create symbolic links.                       |
| McAfee | 1.29.162.1 | CVE-2019-3621 | None               | None       | Authentication protection bypass vulnerability in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.0 allows physical local user to bypass the Windows lock screen via DLPe processes being killed just prior to the screen being locked or when the screen is locked. The attacker requires physical access to the machine. |
| McAfee | 1.29.162.1 | CVE-2019-3635 | MEDIUM             | 6.5        | Exfiltration of Data in McAfee Web Gateway (MWG) 7.8.2.x prior to 7.8.2.12 allows attackers to obtain sensitive data via crafting a complex webpage that will trigger the Web Gateway to block the user accessing an iframe.   |
| McAfee | 1.29.162.1 | CVE-2019-3637 | MEDIUM             | 6.7        | Privilege Escalation vulnerability in McAfee FRP 5.x prior to 5.1.0.209 allows local users to gain elevated privileges via running McAfee Tray with elevated privileges.   |
| McAfee | 1.29.162.1 | CVE-2019-3639 | None               | None       | Clickjack vulnerability in Administrator web console in McAfee Web Gateway (MWG) 7.8.2.x prior to 7.8.2.12 allows remote attackers to conduct clickjacking attacks via a crafted web page that contains an iframe via does not send an X-Frame-Options HTTP header.  |
| McAfee | 1.29.162.1 | CVE-2019-3633 | MEDIUM             | 5.5        | Buffer overflow in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.2.8 allows local user to cause the Windows operating system to "blue screen" via a carefully constructed message sent to DLPe which bypasses DLPe internal checks and results in DLPe reading unallocated memory.                                       |
| McAfee | 1.29.162.1 | CVE-2019-3634 | MEDIUM             | 5.5        | Buffer overflow in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.2.8 allows local user to cause the Windows operating system to "blue screen" via an encrypted message sent to DLPe which when decrypted results in DLPe reading unallocated memory.   |
| McAfee | 1.29.162.1 | CVE-2019-3643 | ['MEDIUM', 'HIGH'] | [5.3, 7.5] | McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9511, potentially leading to a denial of service. This affects the scanning proxies.   |

|        |            |               |                      |            |   |
|--------|------------|---------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2019-3644 | ['HIGH', 'HIGH']     | [7.5, 7.5] | McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9517, potentially leading to a denial of service. This affects the scanning proxies.  |
| McAfee | 1.29.162.1 | CVE-2019-3638 | ['HIGH', 'CRITICAL'] | [8.1, 9.6] | Reflected Cross Site Scripting vulnerability in Administrators web console in McAfee Web Gateway (MWG) 7.8.x prior to 7.8.2.13 allows remote attackers to collect sensitive information or execute commands with the MWG administrator's credentials via tricking the administrator to click on a carefully constructed malicious link. |
| McAfee | 1.29.162.1 | CVE-2019-3646 | ['MEDIUM', 'MEDIUM'] | [6.9, 6.5] | DLL Search Order Hijacking vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Free Antivirus Trial 16.0.R18 and earlier allows local users to execute arbitrary code via execution from a compromised folder placed by an attacker with administrator rights.   |
| McAfee | 1.29.162.1 | CVE-2019-3652 | ['MEDIUM', 'MEDIUM'] | [5.0, 5.3] | Code Injection vulnerability in EPSetup.exe in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to get their malicious code installed by the ENS installer via code injection into EPSetup.exe by an attacker with access to the installer.   |
| McAfee | 1.29.162.1 | CVE-2019-3653 | ['MEDIUM', 'MEDIUM'] | [4.6, 5.5] | Improper access control vulnerability in Configuration tool in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to gain access to security configuration via unauthorized use of the configuration tool.  |
| McAfee | 1.29.162.1 | CVE-2019-3636 | ['HIGH', 'HIGH']     | [7.5, 7.8] | A File Masquerade vulnerability in McAfee Total Protection (MTP) version 16.0.R21 and earlier in Windows client allowed an attacker to read the plaintext list of AV-Scan exclusion files from the Windows registry, and to possibly replace excluded files with potential malware without being detected.                              |
| McAfee | 1.29.162.1 | CVE-2019-3648 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.7] | A Privilege Escalation vulnerability in the Microsoft Windows client in McAfee Total Protection 16.0.R22 and earlier allows administrators to execute arbitrary code via carefully placing malicious files in specific locations protected by administrator permission.   |
| McAfee | 1.29.162.1 | CVE-2019-3641 | ['MEDIUM', 'MEDIUM'] | [4.5, 4.5] | Abuse of Authorization vulnerability in APIs exposed by TIE server in McAfee Threat Intelligence Exchange Server (TIE Server) 3.0.0 allows remote authenticated users to modify stored reputation data via specially crafted messages.  |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2019-3649 | ['MEDIUM', 'MEDIUM'] | [5.3, 6.5] | Information Disclosure vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attackers to gain access to hashed credentials via carefully constructed POST request extracting incorrectly recorded data from log files.   |
| McAfee | 1.29.162.1 | CVE-2019-3650 | ['MEDIUM', 'MEDIUM'] | [5.3, 6.5] | Information Disclosure vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attackers to gain access to the atduser credentials via carefully constructed GET request extracting insecurely information stored in the database.  |
| McAfee | 1.29.162.1 | CVE-2019-3651 | ['HIGH', 'HIGH']     | [8.8, 8.8] | Information Disclosure vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attackers to gain access to ePO as an administrator via using the atduser credentials, which were too permissive.  |
| McAfee | 1.29.162.1 | CVE-2019-3660 | ['HIGH', 'HIGH']     | [8.4, 8.8] | Improper Neutralization of HTTP requests in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attacker to execute commands on the server remotely via carefully constructed HTTP requests.   |
| McAfee | 1.29.162.1 | CVE-2019-3640 | ['MEDIUM', 'MEDIUM'] | [4.8, 6.5] | Unprotected Transport of Credentials in ePO extension in McAfee Data Loss Prevention 11.x prior to 11.4.0 allows remote attackers with access to the network to collect login details to the LDAP server via the ePO extension not using a secure connection when testing LDAP connectivity.   |
| McAfee | 1.29.162.1 | CVE-2019-3661 | ['HIGH', 'HIGH']     | [8.1, 8.8] | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attacker to execute database commands via carefully constructed time based payloads.   |
| McAfee | 1.29.162.1 | CVE-2019-3662 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Path Traversal: '/absolute/pathname/here' vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attacker to gain unintended access to files on the system via carefully constructed HTTP requests.  |
| McAfee | 1.29.162.1 | CVE-2019-3663 | ['CRITICAL', 'HIGH'] | [9.8, 7.8] | Unprotected Storage of Credentials vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows local attacker to gain access to the root password via accessing sensitive files on the system. This was originally published with a CVSS rating of High, further investigation has resulted in this being updated to Critical. The root password is common across all instances of ATD prior to 4.8. See the Security bulletin for further details |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2019-3654 | ['MEDIUM', 'HIGH']   | [5.3, 8.6] | Authentication Bypass vulnerability in the Microsoft Windows client in McAfee Client Proxy (MCP) prior to 3.0.0 allows local user to bypass scanning of web traffic and gain access to blocked sites for a short period of time via generating an authorization key on the client which should only be generated by the network administrator. |
| McAfee | 1.29.162.1 | CVE-2019-3665 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Code Injection vulnerability in the web interface in McAfee Web Advisor (WA) prior to 4.1.1.48 allows remote unauthenticated attacker to allow the browser to render a website which Web Advisor would normally have blocked via a carefully crafted web site.   |
| McAfee | 1.29.162.1 | CVE-2019-3666 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | API Abuse/Misuse vulnerability in the web interface in McAfee Web Advisor (WA) prior to 4.1.1.48 allows remote unauthenticated attacker to allow the browser to navigate to restricted websites via a carefully crafted web site.  |
| McAfee | 1.29.162.1 | CVE-2019-3667 | ['MEDIUM', 'HIGH']   | [6.6, 7.8] | DLL Search Order Hijacking vulnerability in the Microsoft Windows client in McAfee Tech Check 3.0.0.17 and earlier allows local users to execute arbitrary code via the local folder placed there by an attacker.  |
| McAfee | 1.29.162.1 | CVE-2020-7251 | ['MEDIUM', 'MEDIUM'] | [5.0, 5.5] | Improper access control vulnerability in Configuration Tool in McAfee McAfee Endpoint Security (ENS) Prior to 10.6.1 February 2020 Update allows local users to disable security features via unauthorised use of the configuration tool from older versions of ENS.   |
| McAfee | 1.29.162.1 | CVE-2020-7252 | ['MEDIUM', 'MEDIUM'] | [4.2, 5.5] | Unquoted service executable path in DXL Broker in McAfee Data eXchange Layer (DXL) Framework 6.0.0 and earlier allows local users to cause a denial of service and malicious file execution via carefully crafted and named executable files.  |
| McAfee | 1.29.162.1 | CVE-2019-3670 | ['HIGH', 'MEDIUM']   | [8.0, 6.1] | Remote Code Execution vulnerability in the web interface in McAfee Web Advisor (WA) 8.0.34745 and earlier allows remote unauthenticated attacker to execute arbitrary code via a cross site scripting attack.  |
| McAfee | 1.29.162.1 | CVE-2020-7253 | ['MEDIUM', 'MEDIUM'] | [5.7, 4.4] | Improper access control vulnerability in masvc.exe in McAfee Agent (MA) prior to 5.6.4 allows local users with administrator privileges to disable self-protection via a McAfee supplied command-line utility.   |

|        |            |               |                      |            |   |
|--------|------------|---------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2020-7254 | ['HIGH', 'HIGH']     | [7.7, 7.8] | Privilege Escalation vulnerability in the command line interface in McAfee Advanced Threat Defense (ATD) 4.x prior to 4.8.2 allows local users to execute arbitrary code via improper access controls on the sudo command.  |
| McAfee | 1.29.162.1 | CVE-2020-7256 | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update allows attackers to unspecified impact via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2020-7258 | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update allows attackers to unspecified impact via unspecified vectors.  |
| McAfee | 1.29.162.1 | CVE-2020-7260 | ['HIGH', 'HIGH']     | [7.3, 7.8] | DLL Side Loading vulnerability in the installer for McAfee Application and Change Control (MACC) prior to 8.3 allows local users to execute arbitrary code via execution from a compromised folder.   |
| McAfee | 1.29.162.1 | CVE-2020-7263 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.7] | Improper access control vulnerability in ESconfigTool.exe in McAfee Endpoint Security (ENS) for Windows all current versions allows local administrator to alter ENS configuration up to and including disabling all protection offered by ENS via insecurely implemented encryption of configuration for export and import.  |
| McAfee | 1.29.162.1 | CVE-2020-7278 | ['HIGH', 'MEDIUM']   | [7.4, 6.5] | Exploiting incorrectly configured access control security levels vulnerability in ENS Firewall in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 and 10.6.1 April 2020 updates allows remote attackers and local users to allow or block unauthorized traffic via pre-existing rules not being handled correctly when updating to the February 2020 updates. |
| McAfee | 1.29.162.1 | CVE-2020-7257 | ['HIGH', 'MEDIUM']   | [8.4, 6.3] | Privilege escalation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows local users to cause the deletion and creation of files they would not normally have permission to through altering the target of symbolic links whilst an anti-virus scan was in progress. This is timing dependent.                                  |
| McAfee | 1.29.162.1 | CVE-2020-7259 | ['MEDIUM', 'HIGH']   | [6.6, 7.8] | Exploitation of Privilege/Trust vulnerability in file in McAfee Endpoint Security (ENS) Prior to 10.7.0 February 2020 Update allows local users to bypass local security protection via a carefully crafted input file  |

|        |            |               |                      |            |   |
|--------|------------|---------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2020-7261 | ['MEDIUM', 'MEDIUM'] | [6.1, 5.5] | Buffer Overflow via Environment Variables vulnerability in AMSI component in McAfee Endpoint Security (ENS) Prior to 10.7.0 February 2020 Update allows local users to disable Endpoint Security via a carefully crafted user input.  |
| McAfee | 1.29.162.1 | CVE-2020-7273 | ['MEDIUM', 'MEDIUM'] | [6.7, 5.5] | Accessing functionality not properly constrained by ACLs vulnerability in the autorun start-up protection in McAfee Endpoint Security (ENS) for Windows Prior to 10.7.0 April 2020 Update allows local users to delete or rename programs in the autorun key via manipulation of some parameters.   |
| McAfee | 1.29.162.1 | CVE-2020-7274 | ['MEDIUM', 'HIGH']   | [6.6, 7.8] | Privilege escalation vulnerability in McTray.exe in McAfee Endpoint Security (ENS) for Windows Prior to 10.7.0 April 2020 Update allows local users to spawn unrelated processes with elevated privileges via the system administrator granting McTray.exe elevated privileges (by default it runs with the current user's privileges).                                     |
| McAfee | 1.29.162.1 | CVE-2020-7275 | ['MEDIUM', 'MEDIUM'] | [4.8, 5.3] | Accessing, modifying or executing executable files vulnerability in the uninstaller in McAfee Endpoint Security (ENS) for Windows Prior to 10.7.0 April 2020 Update allows local users to execute arbitrary code via a carefully crafted input file.  |
| McAfee | 1.29.162.1 | CVE-2020-7276 | ['MEDIUM', 'MEDIUM'] | [6.4, 6.7] | Authentication bypass vulnerability in MfeUpgradeTool in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 Update allows administrator users to access policy settings via running this tool.   |
| McAfee | 1.29.162.1 | CVE-2020-7277 | ['MEDIUM', 'MEDIUM'] | [6.8, 5.3] | Protection mechanism failure in all processes in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 Update allows local users to stop certain McAfee ENS processes, reducing the protection offered.   |
| McAfee | 1.29.162.1 | CVE-2020-7250 | ['HIGH', 'HIGH']     | [8.2, 7.8] | Symbolic link manipulation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows authenticated local user to potentially gain an escalation of privileges by pointing the link to files which the user which not normally have permission to alter via carefully creating symbolic links from the ENS log file directory. |

|        |            |               |                   |            |   |
|--------|------------|---------------|-------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2020-7255 | ['LOW', 'MEDIUM'] | [3.9, 4.4] | Privilege escalation vulnerability in the administrative user interface in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows local users to gain elevated privileges via ENS not checking user permissions when editing configuration in the ENS client interface. Administrators can lock the ENS client interface through ePO to prevent users being able to edit the configuration. |
| McAfee | 1.29.162.1 | CVE-2020-7264 | ['HIGH', 'HIGH']  | [8.8, 8.4] | Privilege Escalation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 Hotfix 199847 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.   |
| McAfee | 1.29.162.1 | CVE-2020-7265 | ['HIGH', 'HIGH']  | [8.8, 8.4] | Privilege Escalation vulnerability in McAfee Endpoint Security (ENS) for Mac prior to 10.6.9 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.   |
| McAfee | 1.29.162.1 | CVE-2020-7266 | ['HIGH', 'HIGH']  | [8.8, 8.4] | Privilege Escalation vulnerability in McAfee VirusScan Enterprise (VSE) for Windows prior to 8.8 Patch 14 Hotfix 116778 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.                                      |
| McAfee | 1.29.162.1 | CVE-2020-7267 | ['HIGH', 'HIGH']  | [8.8, 8.4] | Privilege Escalation vulnerability in McAfee VirusScan Enterprise (VSE) for Linux prior to 2.0.3 Hotfix 2635000 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.  |
| McAfee | 1.29.162.1 | CVE-2020-7285 | ['HIGH', 'HIGH']  | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee MVISION Endpoint prior to 20.5.0.94 allows a malicious script or program to perform functions that the local executing user has not been granted access to.  |

|        |            |               |                    |            |  |
|--------|------------|---------------|--------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7286 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Exploit Detection and Response (EDR) for Windows prior to 3.1.0 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.  |
| McAfee | 1.29.162.1 | CVE-2020-7287 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Exploit Detection and Response (EDR) for Linux prior to 3.1.0 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.  |
| McAfee | 1.29.162.1 | CVE-2020-7288 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Exploit Detection and Response (EDR) for Mac prior to 3.1.0 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.  |
| McAfee | 1.29.162.1 | CVE-2020-7289 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Active Response (MAR) for Windows prior to 2.4.3 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.   |
| McAfee | 1.29.162.1 | CVE-2020-7290 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Active Response (MAR) for Linux prior to 2.4.3 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.   |
| McAfee | 1.29.162.1 | CVE-2020-7291 | ['HIGH', 'HIGH']   | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Active Response (MAR) for Mac prior to 2.4.3 Hotfix 1 allows a malicious script or program to perform functions that the local executing user has not been granted access to.   |
| McAfee | 1.29.162.1 | CVE-2019-3617 | ['HIGH', 'HIGH']   | [7.5, 8.2] | Privilege escalation vulnerability in McAfee Total Protection (ToPS) for Mac OS prior to 4.6 allows local users to gain root privileges via incorrect protection of temporary files.   |
| McAfee | 1.29.162.1 | CVE-2019-3613 | ['MEDIUM', 'HIGH'] | [5.9, 7.3] | DLL Search Order Hijacking vulnerability in McAfee Agent (MA) prior to 5.6.4 allows attackers with local access to execute arbitrary code via execution from a compromised folder.   |
| McAfee | 1.29.162.1 | CVE-2019-3585 | ['HIGH', 'HIGH']   | [7.0, 7.8] | Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow local users to interact with the On-Access Scan Messages - Threat Alert Window with elevated privileges via running McAfee Tray with elevated privileges. |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2019-3588 | ['MEDIUM', 'MEDIUM'] | [6.3, 6.8] | Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow unauthorized users to interact with the On-Access Scan Messages - Threat Alert Window when the Windows Login Screen is locked.  |
| McAfee | 1.29.162.1 | CVE-2020-7279 | ['MEDIUM', 'HIGH']   | [4.6, 7.8] | DLL Search Order Hijacking Vulnerability in the installer component of McAfee Host Intrusion Prevention System (Host IPS) for Windows prior to 8.0.0 Patch 15 Update allows attackers with local access to execute arbitrary code via execution from a compromised folder.   |
| McAfee | 1.29.162.1 | CVE-2020-7280 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Privilege Escalation vulnerability during daily DAT updates when using McAfee Virus Scan Enterprise (VSE) prior to 8.8 Patch 15 allows local users to cause the deletion and creation of files they would not normally have permission to through altering the target of symbolic links. This is timing dependent.                                   |
| McAfee | 1.29.162.1 | CVE-2020-7262 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.5] | Improper Access Control vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.10.0 allows local users to view sensitive files via a carefully crafted HTTP request parameter.   |
| McAfee | 1.29.162.1 | CVE-2020-7281 | ['HIGH', 'MEDIUM']   | [7.5, 6.3] | Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine. |
| McAfee | 1.29.162.1 | CVE-2020-7282 | ['HIGH', 'MEDIUM']   | [7.5, 6.3] | Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.   |
| McAfee | 1.29.162.1 | CVE-2020-7283 | ['HIGH', 'HIGH']     | [7.5, 8.8] | Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to create and edit files via symbolic link manipulation in a location they would otherwise not have access to. This is achieved through running a malicious script or program on the target machine.  |
| McAfee | 1.29.162.1 | CVE-2020-7284 | ['HIGH', 'HIGH']     | [8.6, 7.8] | Exposure of Sensitive Information in McAfee Network Security Management (NSM) prior to 10.1.7.7 allows local users to gain unauthorised access to the root account via execution of carefully crafted commands from the restricted command line interface (CLI).   |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7292 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Inappropriate Encoding for output context vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows a remote attacker to cause MWG to return an ambiguous redirect response via getting a user to click on a malicious URL.                                |
| McAfee | 1.29.162.1 | CVE-2020-7298 | ['HIGH', 'HIGH']     | [7.5, 8.4] | Unexpected behavior violation in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to turn off real time scanning via a specially crafted object making a specific function call.   |
| McAfee | 1.29.162.1 | CVE-2020-7300 | ['MEDIUM', 'MEDIUM'] | [4.6, 6.3] | Improper Authorization vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote attackers to change the configuration when logged in with view only privileges via carefully constructed HTTP post messages. |
| McAfee | 1.29.162.1 | CVE-2020-7301 | ['MEDIUM', 'MEDIUM'] | [4.1, 4.6] | Cross Site scripting vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated attackers to trigger alerts via the file upload tab in the DLP case management section.   |
| McAfee | 1.29.162.1 | CVE-2020-7302 | ['MEDIUM', 'MEDIUM'] | [5.4, 6.4] | Unrestricted Upload of File with Dangerous Type in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated attackers to upload malicious files to the DLP case management section via lack of sanity checking.                      |
| McAfee | 1.29.162.1 | CVE-2020-7303 | ['MEDIUM', 'MEDIUM'] | [4.1, 4.1] | Cross Site scripting vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote user to trigger scripts to run in a user's browser via adding a new label.   |
| McAfee | 1.29.162.1 | CVE-2020-7304 | ['HIGH', 'HIGH']     | [7.6, 7.6] | Cross site request forgery vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote attacker to embed a CRSF script via adding a new label.  |
| McAfee | 1.29.162.1 | CVE-2020-7305 | ['MEDIUM', 'MEDIUM'] | [6.7, 6.5] | Privilege escalation vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows a low privileged remote attacker to create new rule sets via incorrect validation of user credentials.  |
| McAfee | 1.29.162.1 | CVE-2020-7306 | ['MEDIUM', 'MEDIUM'] | [5.2, 5.2] | Unprotected Storage of Credentials vulnerability in McAfee Data Loss Prevention (DLP) for Mac prior to 11.5.2 allows local users to gain access to the ADRMS username and password via unprotected log files containing plain text                               |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7307 | ['MEDIUM', 'MEDIUM'] | [5.2, 5.2] | Unprotected Storage of Credentials vulnerability in McAfee Data Loss Prevention (DLP) for Mac prior to 11.5.2 allows local users to gain access to the RiskDB username and password via unprotected log files containing plain text credentials.   |
| McAfee | 1.29.162.1 | CVE-2020-7310 | ['MEDIUM', 'MEDIUM'] | [6.9, 6.9] | Privilege Escalation vulnerability in the installer in McAfee McAfee Total Protection (MTP) trial prior to 4.0.161.1 allows local users to change files that are part of write protection rules via manipulating symbolic links to redirect a McAfee file operations to an unintended file.  |
| McAfee | 1.29.162.1 | CVE-2020-7309 | ['LOW', 'MEDIUM']    | [3.9, 4.8] | Cross Site Scripting vulnerability in ePO extension in McAfee Application Control (MAC) prior to 8.3.1 allows administrators to inject arbitrary web script or HTML via specially crafted input in the policy discovery section.   |
| McAfee | 1.29.162.1 | CVE-2020-7299 | ['MEDIUM', 'MEDIUM'] | [5.0, 4.1] | Cleartext Storage of Sensitive Information in Memory vulnerability in Microsoft Windows client in McAfee True Key (TK) prior to 6.2.109.2 allows a local user logged in with administrative privileges to access to another user's passwords on the same machine via triggering a process dump in specific situations.   |
| McAfee | 1.29.162.1 | CVE-2020-7319 | ['HIGH', 'HIGH']     | [8.8, 8.8] | Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local users to access files which the user otherwise would not have access to via manipulating symbolic links to redirect McAfee file operations to an unintended file.   |
| McAfee | 1.29.162.1 | CVE-2020-7320 | ['MEDIUM', 'HIGH']   | [6.7, 7.3] | Protection Mechanism Failure vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local administrator to temporarily reduce the detection capability allowing otherwise detected malware to run via stopping certain Microsoft services.   |
| McAfee | 1.29.162.1 | CVE-2020-7322 | ['MEDIUM', 'MEDIUM'] | [4.7, 4.7] | Information Disclosure Vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local users to gain access to sensitive information via incorrectly logging of sensitive information in debug logs.  |
| McAfee | 1.29.162.1 | CVE-2020-7323 | ['MEDIUM', 'MEDIUM'] | [6.9, 6.9] | Authentication Protection Bypass vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows physical local users to bypass the Windows lock screen via triggering certain detection events while the computer screen is locked and the McTray.exe is running with elevated privileges. This issue is timing dependent and requires physical access to the machine. |

|        |            |               |                          |            |  |
|--------|------------|---------------|--------------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7324 | ['MEDIUM', 'MEDIUM']     | [6.1, 6.1] | Improper Access Control vulnerability in McAfee MVISION Endpoint prior to 20.9 Update allows local users to bypass security mechanisms and deny access to the SYSTEM folder via incorrectly applied permissions.   |
| McAfee | 1.29.162.1 | CVE-2020-7325 | ['MEDIUM', 'HIGH']       | [5.5, 7.8] | Privilege Escalation vulnerability in McAfee MVISION Endpoint prior to 20.9 Update allows local users to access files which the user otherwise would not have access to via manipulating symbolic links to redirect McAfee file operations to an unintended file.  |
| McAfee | 1.29.162.1 | CVE-2020-7311 | ['HIGH', 'HIGH']         | [7.8, 7.0] | Privilege Escalation vulnerability in the installer in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to assume SYSTEM rights during the installation of MA via manipulation of log files.  |
| McAfee | 1.29.162.1 | CVE-2020-7312 | ['HIGH', 'HIGH']         | [7.8, 7.8] | DLL Search Order Hijacking Vulnerability in the installer in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to execute arbitrary code and escalate privileges via execution from a compromised folder.  |
| McAfee | 1.29.162.1 | CVE-2020-7314 | ['HIGH', 'HIGH']         | [8.2, 7.8] | Privilege Escalation Vulnerability in the installer in McAfee Data Exchange Layer (DXL) Client for Mac shipped with McAfee Agent (MA) for Mac prior to MA 5.6.6 allows local users to run commands as root via incorrectly applied permissions on temporary files. |
| McAfee | 1.29.162.1 | CVE-2020-7315 | ['MEDIUM', 'MEDIUM']     | [6.0, 6.7] | DLL Injection Vulnerability in McAfee Agent (MA) for Windows prior to 5.6.6 allows local users to execute arbitrary code via careful placement of a malicious DLL.   |
| McAfee | 1.29.162.1 | CVE-2020-7293 | ['CRITICAL', 'CRITICAL'] | [9.0, 9.0] | Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user with low permissions to change the system's root password via improper access controls in the user interface.                               |
| McAfee | 1.29.162.1 | CVE-2020-7294 | ['MEDIUM', 'MEDIUM']     | [4.6, 4.6] | Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to delete or download protected files via improper access controls in the REST interface.   |
| McAfee | 1.29.162.1 | CVE-2020-7295 | ['LOW', 'MEDIUM']        | [3.5, 4.6] | Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to delete or download protected log data via improper access controls in the user interface.  |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7296 | ['MEDIUM', 'MEDIUM'] | [5.7, 5.7] | Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to access protected configuration files via improper access control in the user interface.  |
| McAfee | 1.29.162.1 | CVE-2020-7297 | ['MEDIUM', 'MEDIUM'] | [5.7, 5.7] | Privilege Escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.1 allows authenticated user interface user to access protected dashboard data via improper access control in the user interface.   |
| McAfee | 1.29.162.1 | CVE-2020-7268 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Path Traversal vulnerability in McAfee McAfee Email Gateway (MEG) prior to 7.6.406 allows remote attackers to traverse the file system to access files or directories that are outside of the restricted directory via external input to construct a path name that should be within a restricted directory.   |
| McAfee | 1.29.162.1 | CVE-2020-7316 | ['MEDIUM', 'HIGH']   | [6.6, 7.8] | Unquoted service path vulnerability in McAfee File and Removable Media Protection (FRP) prior to 5.3.0 allows local users to execute arbitrary code, with higher privileges, via execution and from a compromised folder. This issue may result in files not being encrypted when a policy is triggered.   |
| McAfee | 1.29.162.1 | CVE-2020-7330 | ['HIGH', 'HIGH']     | [7.5, 8.8] | Privilege Escalation vulnerability in McAfee Total Protection (MTP) trial prior to 4.0.176.1 allows local users to schedule tasks which call malicious software to execute with elevated privileges via editing of environment variables   |
| McAfee | 1.29.162.1 | CVE-2020-7317 | ['MEDIUM', 'MEDIUM'] | [4.6, 4.3] | Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10.9 Update 9 allows administrators to inject arbitrary web script or HTML via parameter values for "syncPointList" not being correctly sanitised.  |
| McAfee | 1.29.162.1 | CVE-2020-7318 | ['MEDIUM', 'MEDIUM'] | [4.6, 4.3] | Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10.9 Update 9 allows administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.  |
| McAfee | 1.29.162.1 | CVE-2020-7334 | ['HIGH', 'HIGH']     | [7.7, 8.2] | Improper privilege assignment vulnerability in the installer McAfee Application and Change Control (MACC) prior to 8.3.2 allows local administrators to change or update the configuration settings via a carefully constructed MSI configured to mimic the genuine installer. This version adds further controls for installation/uninstallation of software. |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7326 | ['MEDIUM', 'MEDIUM'] | [6.0, 6.7] | Improperly implemented security check in McAfee Active Response (MAR) prior to 2.4.4 may allow local administrators to execute malicious code via stopping a core Windows service leaving McAfee core trust component in an inconsistent state resulting in MAR failing open rather than closed  |
| McAfee | 1.29.162.1 | CVE-2020-7327 | ['MEDIUM', 'MEDIUM'] | [6.0, 6.7] | Improperly implemented security check in McAfee MVISION Endpoint Detection and Response Client (MVEDR) prior to 3.2.0 may allow local administrators to execute malicious code via stopping a core Windows service leaving McAfee core trust component in an inconsistent state resulting in MVEDR failing open rather than closed       |
| McAfee | 1.29.162.1 | CVE-2020-7328 | ['HIGH', 'HIGH']     | [7.2, 7.2] | External entity attack vulnerability in the ePO extension in McAfee MVISION Endpoint prior to 20.11 allows remote attackers to gain control of a resource or trigger arbitrary code execution via improper input validation of an HTTP request, where the content for the attack has been loaded into ePO by an ePO administrator.       |
| McAfee | 1.29.162.1 | CVE-2020-7329 | ['HIGH', 'HIGH']     | [7.2, 7.2] | Server-side request forgery vulnerability in the ePO extension in McAfee MVISION Endpoint prior to 20.11 allows remote attackers trigger server-side DNS requests to arbitrary domains via carefully constructed XML files loaded by an ePO administrator.   |
| McAfee | 1.29.162.1 | CVE-2020-7331 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Unquoted service executable path in McAfee Endpoint Security (ENS) prior to 10.7.0 November 2020 Update allows local users to cause a denial of service and malicious file execution via carefully crafted and named executable files.   |
| McAfee | 1.29.162.1 | CVE-2020-7332 | ['HIGH', 'HIGH']     | [7.0, 8.8] | Cross Site Request Forgery vulnerability in the firewall ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 November 2020 Update allows an attacker to execute arbitrary HTML code due to incorrect security configuration.   |
| McAfee | 1.29.162.1 | CVE-2020-7333 | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | Cross site scripting vulnerability in the firewall ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 November 2020 Update allows administrators to inject arbitrary web script or HTML via the configuration wizard.   |
| McAfee | 1.29.162.1 | CVE-2020-7335 | ['HIGH', 'HIGH']     | [7.5, 7.8] | Privilege Escalation vulnerability in Microsoft Windows client McAfee Total Protection (MTP) prior to 16.0.29 allows local users to gain elevated privileges via careful manipulation of a folder by creating a junction link. This exploits a lack of protection through a timing issue and is only exploitable in a small time window. |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2020-7337  | ['MEDIUM', 'MEDIUM'] | [6.5, 6.7] | Incorrect Permission Assignment for Critical Resource vulnerability in McAfee VirusScan Enterprise (VSE) prior to 8.8 Patch 16 allows local administrators to bypass local security protection through VSE not correctly integrating with Windows Defender Application Control via careful manipulation of the Code Integrity checks.   |
| McAfee | 1.29.162.1 | CVE-2020-7339  | ['MEDIUM', 'MEDIUM'] | [6.3, 6.3] | Use of a Broken or Risky Cryptographic Algorithm vulnerability in McAfee Database Security Server and Sensor prior to 4.8.0 in the form of a SHA1 signed certificate that would allow an attacker on the same local network to potentially intercept communication between the Server and Sensors.  |
| McAfee | 1.29.162.1 | CVE-2020-7336  | ['MEDIUM', 'MEDIUM'] | [6.6, 6.5] | Cross Site Request Forgery vulnerability in McAfee Network Security Management (NSM) prior to 10.1.7.35 and NSM 9.x prior to 9.2.9.55 may allow an attacker to change the configuration of the Network Security Manager via a carefully crafted HTTP request.   |
| McAfee | 1.29.162.1 | CVE-2020-7343  | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Missing Authorization vulnerability in McAfee Agent (MA) for Windows prior to 5.7.1 allows local users to block McAfee product updates by manipulating a directory used by MA for temporary files. The product would continue to function with out-of-date detection files.   |
| McAfee | 1.29.162.1 | CVE-2021-23878 | ['HIGH', 'MEDIUM']   | [7.3, 5.0] | Clear text storage of sensitive Information in memory vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows a local user to view ENS settings and credentials via accessing process memory after the ENS administrator has performed specific actions. To exploit this, the local user has to access the relevant memory location immediately after an ENS administrator has made a configuration change through the console on their machine |
| McAfee | 1.29.162.1 | CVE-2021-23880 | ['MEDIUM', 'MEDIUM'] | [6.7, 4.4] | Improper Access Control in attribute in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows authenticated local administrator user to perform an uninstallation of the anti-malware engine via the running of a specific command with the correct parameters.  |
| McAfee | 1.29.162.1 | CVE-2021-23882 | ['HIGH', 'MEDIUM']   | [8.2, 4.4] | Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows local administrators to prevent the installation of some ENS files by placing carefully crafted files where ENS will be installed. This is only applicable to clean installations of ENS as the Access Control rules will prevent modification prior to up an upgrade.  |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2021-23883 | ['MEDIUM', 'MEDIUM'] | [4.0, 4.4] | A Null Pointer Dereference vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows a local administrator to cause Windows to crash via a specific system call which is not handled correctly. This varies by machine and had partial protection prior to this update.   |
| McAfee | 1.29.162.1 | CVE-2021-23873 | ['HIGH', 'MEDIUM']   | [7.8, 6.1] | Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and perform arbitrary file deletion as the SYSTEM user potentially causing Denial of Service via manipulating Junction link, after enumerating certain files, at a specific time.  |
| McAfee | 1.29.162.1 | CVE-2021-23874 | ['HIGH', 'HIGH']     | [8.2, 7.8] | Arbitrary Process Execution vulnerability in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and execute arbitrary code bypassing MTP self-defense.  |
| McAfee | 1.29.162.1 | CVE-2021-23876 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Bypass Remote Procedure call in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and perform arbitrary file modification as the SYSTEM user potentially causing Denial of Service via executing carefully constructed malware.  |
| McAfee | 1.29.162.1 | CVE-2021-23881 | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | A stored cross site scripting vulnerability in ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 February 2021 Update allows an ENS ePO administrator to add a script to a policy event which will trigger the script to be run through a browser block page when a local non-administrator user triggers the policy.                                     |
| McAfee | 1.29.162.1 | CVE-2021-23885 | ['CRITICAL', 'HIGH'] | [9.0, 8.8] | Privilege escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.8 allows an authenticated user to gain elevated privileges through the User Interface and execute commands on the appliance via incorrect improper neutralization of user input in the troubleshooting page.  |
| McAfee | 1.29.162.1 | CVE-2021-23879 | ['MEDIUM', 'MEDIUM'] | [6.7, 6.7] | Unquoted service path vulnerability in McAfee Endpoint Product Removal (EPR) Tool prior to 21.2 allows local administrators to execute arbitrary code, with higher-level privileges, via execution from a compromised folder. The tool did not enforce and protect the execution path. Local admin privileges are required to place the files in the required location. |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2020-7346  | ['HIGH', 'HIGH']     | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Data Loss Prevention (DLP) for Windows prior to 11.6.100 allows a local, low privileged, attacker through the use of junctions to cause the product to load DLLs of the attacker's choosing. This requires the creation and removal of junctions by the attacker along with sending a specific IOTL command at the correct time.   |
| McAfee | 1.29.162.1 | CVE-2021-23888 | ['MEDIUM', 'MEDIUM'] | [6.3, 6.3] | Unvalidated client-side URL redirect vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 10 could cause an authenticated ePO user to load an untrusted site in an ePO iframe which could steal information from the authenticated user.   |
| McAfee | 1.29.162.1 | CVE-2021-23889 | ['LOW', 'MEDIUM']    | [3.5, 4.8] | Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 10 allows ePO administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.  |
| McAfee | 1.29.162.1 | CVE-2021-23890 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Information leak vulnerability in the Agent Handler of McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 10 allows an unauthenticated user to download McAfee product packages (specifically McAfee Agent) available in ePO repository and install them on their own machines to have it managed and then in turn get policy details from the ePO server. This can only happen when the ePO Agent Handler is installed in a Demilitarized Zone (DMZ) to service machines not connected to the network through a VPN. |
| McAfee | 1.29.162.1 | CVE-2020-7269  | ['MEDIUM', 'MEDIUM'] | [4.9, 4.3] | Exposure of Sensitive Information in the web interface in McAfee Advanced Threat Defense (ATD) prior to 4.12.2 allows remote authenticated users to view sensitive unencrypted information via a carefully crafted HTTP request parameter. The risk is partially mitigated if your ATD instances are deployed as recommended with no direct access from the Internet to them.   |
| McAfee | 1.29.162.1 | CVE-2020-7270  | ['MEDIUM', 'MEDIUM'] | [4.9, 4.3] | Exposure of Sensitive Information in the web interface in McAfee Advanced Threat Defense (ATD) prior to 4.12.2 allows remote authenticated users to view sensitive unencrypted information via a carefully crafted HTTP request parameter. The risk is partially mitigated if your ATD instances are deployed as recommended with no direct access from the Internet to them.   |

|        |            |                |                      |            |  |
|--------|------------|----------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2020-7308  | ['MEDIUM', 'MEDIUM'] | [4.8, 6.5] | Cleartext Transmission of Sensitive Information between McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update and McAfee Global Threat Intelligence (GTI) servers using DNS allows a remote attacker to view the requests from ENS and responses from GTI over DNS. By gaining control of an intermediate DNS server or altering the network DNS configuration, it is possible for an attacker to intercept requests and send their own responses. |
| McAfee | 1.29.162.1 | CVE-2021-23884 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Cleartext Transmission of Sensitive Information vulnerability in the ePO Extension of McAfee Content Security Reporter (CSR) prior to 2.8.0 allows an ePO administrator to view the unencrypted password of the McAfee Web Gateway (MWG) or the password of the McAfee Web Gateway Cloud Server (MWGCS) read only user used to retrieve log files for analysis in CSR.   |
| McAfee | 1.29.162.1 | CVE-2021-23886 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Denial of Service vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.100 allows a local, low privileged, attacker to cause a BSOD through suspending a process, modifying the processes memory and restarting it. This is triggered by the hdlphook driver reading invalid memory.  |
| McAfee | 1.29.162.1 | CVE-2021-23887 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.100 allows a local, low privileged, attacker to write to arbitrary controlled kernel addresses. This is achieved by launching applications, suspending them, modifying the memory and restarting them when they are monitored by McAfee DLP through the hdlphook driver.  |
| McAfee | 1.29.162.1 | CVE-2021-23872 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Privilege Escalation vulnerability in the File Lock component of McAfee Total Protection (MTP) prior to 16.0.32 allows a local user to gain elevated privileges by manipulating a symbolic link in the IOCTL interface.  |
| McAfee | 1.29.162.1 | CVE-2021-23891 | ['HIGH', 'HIGH']     | [7.8, 7.8] | Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.32 allows a local user to gain elevated privileges by impersonating a client token which could lead to the bypassing of MTP self-defense.  |
| McAfee | 1.29.162.1 | CVE-2021-23894 | ['CRITICAL', 'HIGH'] | [9.6, 8.8] | Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote unauthenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server.   |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2021-23895 | ['CRITICAL', 'HIGH'] | [9.0, 8.0] | Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server.  |
| McAfee | 1.29.162.1 | CVE-2021-23896 | ['LOW', 'MEDIUM']    | [3.2, 4.5] | Cleartext Transmission of Sensitive Information vulnerability in the administrator interface of McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to view the unencrypted password of the McAfee Insights Server used to pass data to the Insights Server. This user is restricted to only have access to DBSec data in the Insights Server.  |
| McAfee | 1.29.162.1 | CVE-2021-31831 | ['MEDIUM', 'MEDIUM'] | [4.9, 5.5] | Incorrect access to deleted scripts vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to gain access to signed SQL scripts which have been marked as deleted or expired within the administrative console. This access was only available through the REST API.   |
| McAfee | 1.29.162.1 | CVE-2021-31830 | ['MEDIUM', 'MEDIUM'] | [5.9, 4.8] | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to embed JavaScript code when configuring the name of a database to be monitored. This would be triggered when any authorized user logs into the DBSec interface and opens the properties configuration page for this database. |
| McAfee | 1.29.162.1 | CVE-2021-31832 | ['MEDIUM', 'MEDIUM'] | [5.2, 4.8] | Improper Neutralization of Input in the ePO administrator extension for McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.200 allows a remote ePO DLP administrator to inject JavaScript code into the alert configuration text field. This JavaScript will be executed when an end user triggers a DLP policy on their machine.   |
| McAfee | 1.29.162.1 | CVE-2021-31837 | ['HIGH', 'HIGH']     | [8.8, 7.8] | Memory corruption vulnerability in the driver file component in McAfee GetSusp prior to 4.0.0 could allow a program being investigated on the local machine to trigger a buffer overflow in GetSusp, leading to the execution of arbitrary code, potentially triggering a BSOD.   |
| McAfee | 1.29.162.1 | CVE-2021-31839 | ['MEDIUM', 'LOW']    | [4.8, 3.3] | Improper privilege management vulnerability in McAfee Agent for Windows prior to 5.7.3 allows a local user to modify event information in the MA event folder. This allows a local user to either add false events or remove events from the event logs prior to them being sent to the ePO server.   |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2021-31840 | ['HIGH', 'HIGH']     | [7.3, 7.3] | A vulnerability in the preloading mechanism of specific dynamic link libraries in McAfee Agent for Windows prior to 5.7.3 could allow an authenticated, local attacker to perform a DLL preloading attack with unsigned DLLs. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. This would result in the user gaining elevated permissions and being able to execute arbitrary code.                                  |
| McAfee | 1.29.162.1 | CVE-2021-31842 | ['MEDIUM', 'MEDIUM'] | [5.0, 5.5] | XML Entity Expansion injection vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2021 Update allows a local user to initiate high CPU and memory consumption resulting in a Denial of Service attack through carefully editing the EPDeploy.xml file and then executing the setup process.  |
| McAfee | 1.29.162.1 | CVE-2021-31843 | ['HIGH', 'HIGH']     | [7.3, 7.8] | Improper privileges management vulnerability in McAfee Endpoint Security (ENS) Windows prior to 10.7.0 September 2021 Update allows local users to access files which they would otherwise not have access to via manipulating junction links to redirect McAfee folder operations to an unintended location.   |
| McAfee | 1.29.162.1 | CVE-2021-31844 | ['HIGH', 'HIGH']     | [8.2, 7.3] | A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.200 allows a local attacker to execute arbitrary code with elevated privileges through placing carefully constructed Ami Pro (.sam) files onto the local system and triggering a DLP Endpoint scan through accessing a file. This is caused by the destination buffer being of fixed size and incorrect checks being made on the source size.                       |
| McAfee | 1.29.162.1 | CVE-2021-31845 | ['HIGH', 'HIGH']     | [8.4, 7.3] | A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Discover prior to 11.6.100 allows an attacker in the same network as the DLP Discover to execute arbitrary code through placing carefully constructed Ami Pro (.sam) files onto a machine and having DLP Discover scan it, leading to remote code execution with elevated privileges. This is caused by the destination buffer being of fixed size and incorrect checks being made on the source size. |
| McAfee | 1.29.162.1 | CVE-2021-31836 | ['MEDIUM', 'HIGH']   | [5.6, 7.1] | Improper privilege management vulnerability in maconfig for McAfee Agent for Windows prior to 5.7.4 allows a local user to gain access to sensitive information. The utility was able to be run from any location on the file system and by a low privileged user.  |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2021-31841 | ['HIGH', 'HIGH']     | [8.2, 7.3] | A DLL sideloading vulnerability in McAfee Agent for Windows prior to 5.7.4 could allow a local user to perform a DLL sideloading attack with an unsigned DLL with a specific name and in a specific location. This would result in the user gaining elevated permissions and the ability to execute arbitrary code as the system user, through not checking the DLL signature.  |
| McAfee | 1.29.162.1 | CVE-2021-31847 | ['HIGH', 'HIGH']     | [8.2, 7.8] | Improper access control vulnerability in the repair process for McAfee Agent for Windows prior to 5.7.4 could allow a local attacker to perform a DLL preloading attack using unsigned DLLs. This would result in elevation of privileges and the ability to execute arbitrary code as the system user, through not correctly protecting a temporary directory used in the repair process and not checking the DLL signature. |
| McAfee | 1.29.162.1 | CVE-2021-23893 | ['HIGH', 'HIGH']     | [8.8, 7.8] | Privilege Escalation vulnerability in a Windows system driver of McAfee Drive Encryption (DE) prior to 7.3.0 could allow a local non-admin user to gain elevated system privileges via exploiting an unutilized memory buffer.  |
| McAfee | 1.29.162.1 | CVE-2021-31834 | MEDIUM               | 5.4        | Stored Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.   |
| McAfee | 1.29.162.1 | CVE-2021-31835 | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via a specific parameter where the administrator's entries were not correctly sanitized.   |
| McAfee | 1.29.162.1 | CVE-2021-23877 | ['MEDIUM', 'HIGH']   | [6.7, 7.8] | Privilege escalation vulnerability in the Windows trial installer of McAfee Total Protection (MTP) prior to 16.0.34_x may allow a local user to run arbitrary code as the admin user by replacing a specific temporary file created during the installation of the trial version of MTP.  |
| McAfee | 1.29.162.1 | CVE-2021-31848 | ['HIGH', 'MEDIUM']   | [8.4, 6.1] | Cross site scripting (XSS) vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker to highjack an active DLP ePO administrator session by convincing the logged in administrator to click on a carefully crafted link in the case management part of the DLP ePO extension.   |

|        |            |                |                      |            |  |
|--------|------------|----------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2021-31849 | ['HIGH', 'HIGH']     | [8.4, 7.2] | SQL injection vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker logged into ePO as an administrator to inject arbitrary SQL into the ePO database through the user management section of the DLP ePO extension.  |
| McAfee | 1.29.162.1 | CVE-2021-31853 | ['HIGH', 'HIGH']     | [7.8, 7.8] | DLL Search Order Hijacking Vulnerability in McAfee Drive Encryption (MDE) prior to 7.3.0 HF2 (7.3.0.183) allows local users to execute arbitrary code and escalate privileges via execution from a compromised folder.   |
| McAfee | 1.29.162.1 | CVE-2021-31851 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | A Reflected Cross-Site Scripting vulnerability in McAfee Policy Auditor prior to 6.5.2 allows a remote unauthenticated attacker to inject arbitrary web script or HTML via the profileNodeID request parameters. The malicious script is reflected unmodified into the Policy Auditor web-based interface which could lead to the extraction of end user session token or login credentials. These may be used to access additional security-critical applications or conduct arbitrary cross-domain requests. |
| McAfee | 1.29.162.1 | CVE-2021-31852 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | A Reflected Cross-Site Scripting vulnerability in McAfee Policy Auditor prior to 6.5.2 allows a remote unauthenticated attacker to inject arbitrary web script or HTML via the UID request parameter. The malicious script is reflected unmodified into the Policy Auditor web-based interface which could lead to the extract of end user session token or login credentials. These may be used to access additional security-critical applications or conduct arbitrary cross-domain requests.               |
| McAfee | 1.29.162.1 | CVE-2021-4038  | ['MEDIUM', 'MEDIUM'] | [4.8, 4.8] | Cross Site Scripting (XSS) vulnerability in McAfee Network Security Manager (NSM) prior to 10.1 Minor 7 allows a remote authenticated administrator to embed a XSS in the administrator interface via specially crafted custom rules containing HTML. NSM did not correctly sanitize custom rule content in all scenarios.   |
| McAfee | 1.29.162.1 | CVE-2021-31833 | ['HIGH', 'HIGH']     | [7.1, 7.8] | Potential product security bypass vulnerability in McAfee Application and Change Control (MACC) prior to version 8.3.4 allows a locally logged in attacker to circumvent the application solidification protection provided by MACC, permitting them to run applications that would usually be prevented by MACC. This would require the attacker to rename the specified binary to match name of any configured updater and perform a specific set of steps, resulting in the renamed binary to be to run.    |

|        |            |                |                      |            |  |
|--------|------------|----------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2022-0129  | ['HIGH', 'MEDIUM']   | [7.4, 6.7] | Uncontrolled search path element vulnerability in McAfee TechCheck prior to 4.0.0.2 allows a local administrator to load their own Dynamic Link Library (DLL) gaining elevation of privileges to system user. This was achieved through placing the malicious DLL in the same directory that the process was run from.   |
| McAfee | 1.29.162.1 | CVE-2021-31854 | ['HIGH', 'HIGH']     | [7.7, 7.8] | A command Injection Vulnerability in McAfee Agent (MA) for Windows prior to 5.7.5 allows local users to inject arbitrary shell code into the file cleanup.exe. The malicious clean.exe file is placed into the relevant folder and executed by running the McAfee Agent deployment feature located in the System Tree. An attacker may exploit the vulnerability to obtain a reverse shell which can lead to privilege escalation to obtain root privileges. |
| McAfee | 1.29.162.1 | CVE-2022-0166  | ['HIGH', 'HIGH']     | [7.8, 7.8] | A privilege escalation vulnerability in the McAfee Agent prior to 5.7.5. McAfee Agent uses openssl.cnf during the build process to specify the OPENSSLDIR variable as a subdirectory within the installation directory. A low privilege user could have created subdirectories and executed arbitrary code with SYSTEM privileges by creating the appropriate pathway to the specifically created malicious openssl.cnf file.                                |
| McAfee | 1.29.162.1 | CVE-2022-0280  | ['HIGH', 'HIGH']     | [7.5, 7.0] | A race condition vulnerability exists in the QuickClean feature of McAfee Total Protection for Windows prior to 16.0.43 that allows a local user to gain privilege elevation and perform an arbitrary file delete. This could lead to sensitive files being deleted and potentially cause denial of service. This attack exploits the way symlinks are created and how the product works with them.  |
| McAfee | 1.29.162.1 | CVE-2022-0815  | ['MEDIUM', 'HIGH']   | [6.5, 7.3] | Improper access control vulnerability in McAfee WebAdvisor Chrome and Edge browser extensions up to 8.1.0.1895 allows a remote attacker to gain access to McAfee WebAdvisor settings and other details about the user's system. This could lead to unexpected behaviors including; settings being changed, fingerprinting of the system leading to targeted scams, and not triggering the malicious software if McAfee software is detected.                 |
| McAfee | 1.29.162.1 | CVE-2022-0842  | ['MEDIUM', 'MEDIUM'] | [5.4, 4.9] | A blind SQL injection vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote authenticated attacker to potentially obtain information from the ePO database. The data obtained is dependent on the privileges the attacker has and to obtain sensitive data the attacker would require administrator privileges.  |

|        |            |               |                      |            |  |
|--------|------------|---------------|----------------------|------------|--|
| McAfee | 1.29.162.1 | CVE-2022-0857 | ['MEDIUM', 'MEDIUM'] | [5.4, 6.1] | A reflected cross-site scripting (XSS) vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to potentially obtain access to an ePO administrator's session by convincing the attacker to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO due to the area of the User Interface the vulnerability is present in.                         |
| McAfee | 1.29.162.1 | CVE-2022-0858 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.7] | A cross-site scripting (XSS) vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to potentially obtain access to an ePO administrator's session by convincing the attacker to click on a carefully crafted link. This would lead to limited ability to alter some information in ePO due to the area of the User Interface the vulnerability is present in.   |
| McAfee | 1.29.162.1 | CVE-2022-0859 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.7] | McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a local attacker to point an ePO server to an arbitrary SQL server during the restoration of the ePO server. To achieve this the attacker would have to be logged onto the server hosting the ePO server (restricted to administrators) and to know the SQL server password.   |
| McAfee | 1.29.162.1 | CVE-2022-0861 | ['LOW', 'LOW']       | [3.5, 3.8] | A XML Extended entity vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote administrator attacker to upload a malicious XML file through the extension import functionality. The impact is limited to some access to confidential information and some ability to alter data.   |
| McAfee | 1.29.162.1 | CVE-2022-0862 | ['LOW', 'MEDIUM']    | [3.1, 5.3] | A lack of password change protection vulnerability in a deprecated API of McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to change the password of a compromised session without knowing the existing user's password. This functionality was removed from the User Interface in ePO 10 and the API has now been disabled. Other protection is in place to reduce the likelihood of this being successful through sending a link to a logged in user. |
| McAfee | 1.29.162.1 | CVE-2022-1823 | ['HIGH', 'HIGH']     | [7.9, 7.8] | Improper privilege management vulnerability in McAfee Consumer Product Removal Tool prior to version 10.4.128 could allow a local user to modify a configuration file and perform a LOLBin (Living off the land) attack. This could result in the user gaining elevated permissions and being able to execute arbitrary code, through not correctly checking the integrity of the configuration file.  |

|        |            |                |                      |            |   |
|--------|------------|----------------|----------------------|------------|---|
| McAfee | 1.29.162.1 | CVE-2022-1824  | ['HIGH', 'HIGH']     | [7.9, 8.2] | An uncontrolled search path vulnerability in McAfee Consumer Product Removal Tool prior to version 10.4.128 could allow a local attacker to perform a sideloading attack by using a specific file name. This could result in the user gaining elevated permissions and being able to execute arbitrary code as there were insufficient checks on the executable being signed by McAfee. |
| McAfee | 1.29.162.1 | CVE-2022-37025 | HIGH                 | 7.8        | An improper privilege management vulnerability in McAfee Security Scan Plus (MSS+) before 4.1.262.1 could allow a local user to modify a configuration file and perform a LOLBin (Living off the land) attack. This could result in the user gaining elevated permissions and being able to execute arbitrary code due to lack of an integrity check of the configuration file.         |
| McAfee | 1.29.162.1 | CVE-2022-43751 | ['HIGH', 'HIGH']     | [7.8, 7.8] | McAfee Total Protection prior to version 16.0.49 contains an uncontrolled search path element vulnerability due to the use of a variable pointing to a subdirectory that may be controllable by an unprivileged user. This may have allowed the unprivileged user to execute arbitrary code with system privileges.   |
| McAfee | 1.29.162.1 | CVE-2023-24577 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | McAfee Total Protection prior to 16.0.50 allows attackers to elevate user privileges due to Improper Link Resolution via registry keys. This could enable a user with lower privileges to execute unauthorized tasks.   |
| McAfee | 1.29.162.1 | CVE-2023-24578 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | McAfee Total Protection prior to 16.0.49 allows attackers to elevate user privileges due to DLL sideloading. This could enable a user with lower privileges to execute unauthorized tasks.  |
| McAfee | 1.29.162.1 | CVE-2023-24579 | ['MEDIUM', 'HIGH']   | [5.5, 7.8] | McAfee Total Protection prior to 16.0.51 allows attackers to trick a victim into uninstalling the application via the command prompt.   |
| McAfee | 1.29.162.1 | CVE-2023-25134 | ['MEDIUM', 'MEDIUM'] | [6.7, 6.7] | McAfee Total Protection prior to 16.0.50 may allow an adversary (with full administrative access) to modify a McAfee specific Component Object Model (COM) in the Windows Registry. This can result in the loading of a malicious payload.  |
| McAfee | 1.29.162.1 | CVE-2023-40352 | HIGH                 | 7.2        | McAfee Safe Connect before 2.16.1.126 may allow an adversary with system privileges to achieve privilege escalation by loading arbitrary DLLs.  |
| McAfee | 1.29.162.1 | CVE-2024-34405 | CRITICAL             | 9.1        | Improper deep link validation in McAfee Security: Antivirus VPN for Android before 8.3.0 could allow an attacker to launch an arbitrary URL within the app.   |

|                |                   |                |        |      |   |
|----------------|-------------------|----------------|--------|------|---|
| McAfee         | 1.29.162.1        | CVE-2024-34406 | MEDIUM | 5.3  | Improper exception handling in McAfee Security: Antivirus VPN for Android before 8.3.0 could allow an attacker to cause a denial of service through the use of a malformed deep link.   |
| McAfee         | 1.29.162.1        | CVE-2024-49592 | MEDIUM | 6.7  | Trial installer for McAfee Total Protection (legacy trial installer software) 16.0.53 allows local privilege escalation because of an Uncontrolled Search Path Element. The attacker could be "an adversary or knowledgeable user" and the type of attack could be called "DLL-squatting." The issue only affects execution of this installer, and does not leave McAfee Total Protection in a vulnerable state after installation is completed. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2441  | None   | None | Microsoft Internet Explorer 7 through 11 and Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2452.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2442  | None   | None | Microsoft Internet Explorer 8 through 11 and Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2444.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2446  | None   | None | Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2447.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2449  | None   | None | Microsoft Internet Explorer 7 through 11 and Edge allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "ASLR Bypass."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2485  | None   | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2491 and CVE-2015-2541.  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2486 | None | None | Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.                        |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2494 | None | None | Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2498, and CVE-2015-2499.                        |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-2542 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6057 | None | None | Microsoft Edge allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6058 | None | None | Microsoft Edge mishandles HTML attributes in HTTP responses, which allows remote attackers to bypass a cross-site scripting (XSS) protection mechanism via unspecified vectors, aka "Microsoft Edge XSS Filter Bypass."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6064 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6084 and CVE-2015-6085.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6073 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6078 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6065.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6088 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Microsoft Browser ASLR Bypass."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6139 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge mishandle content types, which allows remote attackers to execute arbitrary web script in a privileged context via a crafted web site, aka "Microsoft Browser Elevation of Privilege Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6140 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6142 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6144 | None | None | Microsoft Internet Explorer 8 through 11 and Microsoft Edge mishandle HTML attributes in HTTP responses, which allows remote attackers to bypass a cross-site scripting (XSS) protection mechanism via unspecified vectors, aka "Microsoft Browser XSS Filter Bypass Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6148 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6156.  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6151 | None | None | Microsoft Internet Explorer 8 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6083.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6153 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6154 | None | None | Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6150.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6155 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6158 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6159, and CVE-2015-6160. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6159 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, and CVE-2015-6160. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6161 | None | None | Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Microsoft Browser ASLR Bypass."   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6168 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6153.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6169 | None | None | Microsoft Edge misparses HTTP responses, which allows remote attackers to redirect users to arbitrary web sites via unspecified vectors, aka "Microsoft Edge Spoofing Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6170 | None | None | Microsoft Edge allows remote attackers to gain privileges via a crafted web site, aka "Microsoft Browser Elevation of Privilege Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2015-6176 | None | None | Microsoft Edge mishandles HTML attributes in HTTP responses, which allows remote attackers to bypass a cross-site scripting (XSS) protection mechanism via unspecified vectors, aka "Microsoft Edge XSS Filter Bypass Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0003 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code via unspecified vectors, aka "Microsoft Edge Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0024 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via unspecified vectors, aka "Scripting Engine Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0060 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0061, CVE-2016-0063, CVE-2016-0067, and CVE-2016-0072. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0061 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0060, CVE-2016-0063, CVE-2016-0067, and CVE-2016-0072. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0062 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0077 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge misparse HTTP responses, which allows remote attackers to spoof web sites via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0080 | None | None | Microsoft Edge mishandles exceptions during window-message dispatch operations, which allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Microsoft Edge ASLR Bypass."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0084 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0102 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0105 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0107, CVE-2016-0111, CVE-2016-0112, and CVE-2016-0113.      |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0109 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, and CVE-2016-0114. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0110 | None | None | Microsoft Internet Explorer 10 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0111 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0112, and CVE-2016-0113. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0116 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0123, CVE-2016-0124, CVE-2016-0129, and CVE-2016-0130.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0123 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0124, CVE-2016-0129, and CVE-2016-0130.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0124 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0129, and CVE-2016-0130.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0125 | None | None | Microsoft Edge mishandles the Referer policy, which allows remote attackers to obtain sensitive browser-history and request information via a crafted HTTPS web site, aka "Microsoft Edge Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0129 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, and CVE-2016-0130.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0130 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, and CVE-2016-0129.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0154 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0155 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0156 and CVE-2016-0157.                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0156 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0157.                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0157 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0156.                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0158 | None | None | Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Edge Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0161.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0161 | None | None | Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Edge Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0158.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0186 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0191 and CVE-2016-0193. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0191 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0186 and CVE-2016-0193. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0192 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0193 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0186 and CVE-2016-0191. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1096 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1097 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1098 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1099 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1100 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1101 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1102 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.                    |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1103 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1104 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1105 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1106 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1107 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1108 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1109 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-1110 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4108 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4109 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4110 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4111 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4112 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4113 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4114 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4115 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4116 | None | None | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3198 | None | None | Microsoft Edge allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a crafted document, aka "Microsoft Edge Security Feature Bypass."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3199 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3214.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3201 | None | None | Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka "Windows PDF Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3215.                  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3202 | None | None | The Microsoft (1) Chakra JavaScript, (2) JScript, and (3) VBScript engines, as used in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3203 | None | None | Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to execute arbitrary code via a crafted PDF document, aka "Windows PDF Remote Code Execution Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3214 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3199.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3215 | None | None | Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka "Windows PDF Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3201.                           |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3222 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4122 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4123 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4124 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4125 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4126 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4127 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4128 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |

|                |                   |               |      |     |  |
|----------------|-------------------|---------------|------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4129 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4130 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4131 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4132 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4133 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4134 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4135 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4136 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |

|                |                   |               |          |     |  |
|----------------|-------------------|---------------|----------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4137 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4138 | CRITICAL | 9.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4139 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4140 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4141 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4142 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4143 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4144 | HIGH     | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |

|                |                   |               |      |     |  |
|----------------|-------------------|---------------|------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4145 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4146 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4147 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4148 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4149 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4150 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4151 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4152 | HIGH | 8.8 | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4153 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4154 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4155 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4156 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-4166 | HIGH | 8.8  | Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3244 | None | None | Microsoft Edge allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Microsoft Edge Security Feature Bypass."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3246 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3248 | None | None | The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3259. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3259 | None | None | The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3248. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3260 | None | None | The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3264 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3265 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3269.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3269 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3265.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3271 | None | None | The VBScript engine in Microsoft Edge allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3273 | None | None | The XSS Filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge does not properly restrict JavaScript code, which allows remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3274 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3276 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3277 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3289 | None | None | Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3322.                                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3293 | None | None | Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3296 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3319 | None | None | The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allows remote attackers to execute arbitrary code via a crafted PDF file, aka "Microsoft PDF Remote Code Execution Vulnerability." |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3322 | None | None | Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3289.                                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3326 | None | None | Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3327.               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3327 | None | None | Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3326.               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3329 | None | None | Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to determine the existence of files via a crafted webpage, aka "Internet Explorer Information Disclosure Vulnerability."  |

|                |                   |               |                         |               |   |
|----------------|-------------------|---------------|-------------------------|---------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3247 | None                    | None          | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3291 | None                    | None          | Microsoft Internet Explorer 11 and Microsoft Edge mishandle cross-origin requests, which allows remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3294 | None                    | None          | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3330.                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3295 | None                    | None          | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."                                     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3297 | None                    | None          | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."                                  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3325 | None                    | None          | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3330 | None                    | None          | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3294.                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3350 | None                    | None          | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3377. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3351 | ['MEDIUM',<br>'MEDIUM'] | [6.5,<br>6.5] | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3370 | None | None | The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3374. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3374 | None | None | The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3370. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3377 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3350.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3267 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to determine the existence of unspecified files via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3331 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3382 | None | None | The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as demonstrated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerability."    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3386 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3389, CVE-2016-7190, and CVE-2016-7194.          |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3387 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private namespaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Browser Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3388.             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3388 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private namespaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Browser Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3387.             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3389 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-7190, and CVE-2016-7194. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3390 | None | None | The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as demonstrated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerability."     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3391 | None | None | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow context-dependent attackers to discover credentials by leveraging access to a memory dump, aka "Microsoft Browser Information Disclosure Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-3392 | None | None | The Edge Content Security Policy feature in Microsoft Edge does not properly validate documents, which allows remote attackers to bypass intended access restrictions via a crafted web site, aka "Microsoft Browser Security Feature Bypass Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7189 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Remote Code Execution Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7190 | None | None | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-3389, and CVE-2016-7194. |

|                |                   |               |                  |            |   |
|----------------|-------------------|---------------|------------------|------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7194 | None             | None       | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-3389, and CVE-2016-7190.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7195 | None             | None       | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7198.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7196 | None             | None       | Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7198 | None             | None       | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7195.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7199 | None             | None       | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the Same Origin Policy and obtain sensitive window-state information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7200 | ['HIGH', 'HIGH'] | [8.8, 8.8] | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7201 | ['HIGH', 'HIGH'] | [8.8, 8.8] | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7202 | None | None | The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," as demonstrated by the Chakra JavaScript engine, a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7203 | None | None | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7204 | None | None | Microsoft Edge allows remote attackers to access arbitrary "My Documents" files via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7208 | None | None | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7209 | None | None | Microsoft Edge allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7227 | None | None | The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to determine the existence of local files via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7239 | None | None | The RegEx class in the XSS filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to conduct cross-site scripting (XSS) attacks and obtain sensitive information via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7240 | None | None | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7242, and CVE-2016-7243. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7241 | None | None | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7242 | None | None | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, and CVE-2016-7243. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7243 | None | None | The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, and CVE-2016-7242. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7181 | None | None | Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7206 | None | None | Cross-site scripting (XSS) vulnerability in Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7280.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7279 | None | None | Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7280 | None | None | Cross-site scripting (XSS) vulnerability in Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7206.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7281 | None | None | The Web Workers implementation in Microsoft Internet Explorer 10 and 11 and Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Browser Security Feature Bypass Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7282 | None | None | Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7286 | None | None | The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7288, CVE-2016-7296, and CVE-2016-7297. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7287 | None | None | The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7288 | None | None | The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7296, and CVE-2016-7297. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7296 | None | None | The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7288, and CVE-2016-7297. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-7297 | None | None | The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7288, and CVE-2016-7296. |

|                |                   |               |                  |            |  |
|----------------|-------------------|---------------|------------------|------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0002 | None             | None       | Microsoft Edge allows remote attackers to bypass the Same Origin Policy via vectors involving the about:blank URL and data: URLs, aka "Microsoft Edge Elevation of Privilege Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0037 | ['HIGH', 'HIGH'] | [8.1, 8.1] | Microsoft Internet Explorer 10 and 11 and Microsoft Edge have a type confusion issue in the Layout::MultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement function in mshtml.dll, which allows remote attackers to execute arbitrary code via vectors involving a crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code that operates on a TH element. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0011 | None             | None       | Microsoft Edge allows remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0017, CVE-2017-0065, and CVE-2017-0068.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0012 | None             | None       | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a crafted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those described in CVE-2017-0033 and CVE-2017-0069.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0017 | None             | None       | The RegEx class in the XSS filter in Microsoft Edge allows remote attackers to conduct cross-site scripting (XSS) attacks and obtain sensitive information via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0011, CVE-2017-0065, and CVE-2017-0068.                     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0023 | None             | None       | The PDF library in Microsoft Edge; Windows 8.1; Windows Server 2012 and R2; Windows RT 8.1; and Windows 10, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted PDF file, aka "Microsoft PDF Remote Code Execution Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0033 | None             | None       | Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a crafted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those described in CVE-2017-0012 and CVE-2017-0069.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0034 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0065 | None | None | Microsoft Edge allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0011, CVE-2017-0017, and CVE-2017-0068.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0066 | None | None | Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka "Microsoft Edge Security Feature Bypass Vulnerability." This vulnerability is different from those described in CVE-2017-0135 and CVE-2017-0140.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0068 | None | None | Browsers in Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0011, CVE-2017-0017, and CVE-2017-0065.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0069 | None | None | Microsoft Edge allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing Vulnerability." This vulnerability is different from those described in CVE-2017-0012 and CVE-2017-0033.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0135 | None | None | Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka "Microsoft Edge Security Feature Bypass Vulnerability." This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0140.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0140 | None | None | Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka "Microsoft Edge Security Feature Bypass Vulnerability." This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0135.  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0093 | None | None | A remote code execution vulnerability in Microsoft Edge exists in the way that the Scripting Engine renders when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0201. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0200 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user, aka "Microsoft Edge Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0203 | None | None | A vulnerability exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. An attacker could trick a user into loading a web page with malicious content, aka "Microsoft Edge Security Feature Bypass Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0205 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user, aka "Microsoft Edge Memory Corruption Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0208 | None | None | An information disclosure vulnerability exists in Microsoft Edge when the Chakra scripting engine does not properly handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system, a.k.a. "Scripting Engine Information Disclosure Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0221 | None | None | A vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0227 and CVE-2017-0240.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0224 | None | None | A remote code execution vulnerability exists in the way JavaScript engines render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0228, CVE-2017-0229, CVE-2017-0230, CVE-2017-0234, CVE-2017-0235, CVE-2017-0236, and CVE-2017-0238.  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0227 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0221 and CVE-2017-0240.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0229 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way JavaScript engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0224, CVE-2017-0228, CVE-2017-0230, CVE-2017-0234, CVE-2017-0235, CVE-2017-0236, and CVE-2017-0238.                 |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0230 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way JavaScript engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0224, CVE-2017-0228, CVE-2017-0229, CVE-2017-0234, CVE-2017-0235, CVE-2017-0236, and CVE-2017-0238.                 |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0233 | None | None | An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft Edge Elevation of Privilege Vulnerability." This CVE ID is unique from CVE-2017-0241.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0234 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way that the Chakra JavaScript engine renders when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0224, CVE-2017-0228, CVE-2017-0229, CVE-2017-0230, CVE-2017-0235, CVE-2017-0236, and CVE-2017-0238. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0235 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way that the Chakra JavaScript engine renders when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0224, CVE-2017-0228, CVE-2017-0229, CVE-2017-0230, CVE-2017-0234, CVE-2017-0236, and CVE-2017-0238. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0236 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way that the Chakra JavaScript engine renders when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0224, CVE-2017-0228, CVE-2017-0229, CVE-2017-0230, CVE-2017-0234, CVE-2017-0235, and CVE-2017-0238.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0240 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0221 and CVE-2017-0227.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0241 | None | None | An elevation of privilege vulnerability exists when Microsoft Edge renders a domain-less page in the URL, which could allow Microsoft Edge to perform actions in the context of the Intranet Zone and access functionality that is not typically available to the browser when browsing in the context of the Internet Zone, aka "Microsoft Edge Elevation of Privilege Vulnerability." This CVE ID is unique from CVE-2017-0233. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-0266 | None | None | A remote code execution vulnerability exists in Microsoft Edge in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Remote Code Execution Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8496 | None | None | Microsoft Edge in Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8497.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8497 | None | None | Microsoft Edge in Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8496.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8498 | None | None | Microsoft Edge in Windows 10 1607 and 1703, and Windows Server 2016 allows an attacker to read data not intended to be disclosed when Edge allows JavaScript XML DOM objects to detect installed browser extensions, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8504.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8499 | None | None | Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8520, CVE-2017-8521, CVE-2017-8548, and CVE-2017-8549.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8504 | None | None | Microsoft Edge in Windows 10 1607 and 1703, and Windows Server 2016 allows an attacker to read the URL of a cross-origin request when the Microsoft Edge Fetch API incorrectly handles a filtered response type, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8498.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8520 | None | None | Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8499, CVE-2017-8521, CVE-2017-8548, and CVE-2017-8549.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8521 | None | None | Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8548, and CVE-2017-8549.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8523 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when Microsoft Edge fails to correctly apply Same Origin Policy for HTML elements present in other browser windows, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-8530 and CVE-2017-8555. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8530 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when Microsoft Edge does not properly enforce same-origin policies, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-8523 and CVE-2017-8555.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8548 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8549.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8549 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8548.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8555 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-8523 and CVE-2017-8530.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2016-0959 | None | None | Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8595 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8596 | None | None | Microsoft Edge in Microsoft Windows 10 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8610, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8598 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8599 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka "Microsoft Edge Security Feature Bypass Vulnerability".  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8601 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8598 and CVE-2017-8609.                 |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8603 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8598, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8604 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8610, CVE-2017-8603, CVE-2017-8598, CVE-2017-8601, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8605 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8598, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8610 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8595, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8611 | None | None | Microsoft Edge on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing Vulnerability."  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8617 | None | None | Microsoft Edge in Windows 10 1703 Microsoft Edge allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Remote Code Execution Vulnerability."   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8619 | None | None | Microsoft Edge on Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8618, CVE-2017-9598 and CVE-2017-8609.                     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8503 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to escape from the AppContainer sandbox, aka "Microsoft Edge Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8642.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8634 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.                      |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8637 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to bypass Arbitrary Code Guard (ACG) due to how Microsoft Edge accesses memory in code compiled by the Edge Just-In-Time (JIT) compiler, aka "Scripting Engine Security Feature Bypass Vulnerability".  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8638 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.                      |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8639 | None | None | Microsoft Edge in Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8640 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8642 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to elevate privileges due to the way that Microsoft Edge validates JavaScript under specific conditions, aka "Microsoft Edge Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8503.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8644 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to disclose information due to the way that Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8652 and CVE-2017-8662.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8645 | None | None | Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.       |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8646 | None | None | Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.                 |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8647 | None | None | Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8650 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to exploit a security feature bypass due to Microsoft Edge not properly enforcing same-origin policies, aka "Microsoft Edge Security Feature Bypass Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8652 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to disclose information due to the way that Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8644 and CVE-2017-8662.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8655 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8656 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8657 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8659 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system due to the Chakra scripting engine not properly handling objects in memory, aka "Scripting Engine Information Disclosure Vulnerability".  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8661 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8662 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to disclose information due to how strings are validated in specific scenarios, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8644 and CVE-2017-8652.  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8670 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8671 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8672, and CVE-2017-8674. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8672 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, and CVE-2017-8674. |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8674  | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, and CVE-2017-8672. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8518  | None | None | Microsoft Edge allows a remote code execution vulnerability due to the way it accesses objects in memory, aka "Scripting Engine Memory Corruption Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11764 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-8756.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11766 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-8751.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8597  | None | None | Microsoft Edge in Microsoft Windows 10 Version 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8643 and CVE-2017-8648.  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8643 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to leave a malicious website open during user clipboard activities, due to the way that Microsoft Edge handles clipboard events, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8597 and CVE-2017-8648.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8648 | None | None | Microsoft Edge in Microsoft Windows Version 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8597 and CVE-2017-8643.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8649 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8660 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8723 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page containing malicious content, due to the way that the Edge Content Security Policy (CSP) validates certain specially crafted documents, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-8754.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8724 | None | None | Microsoft Edge in Microsoft Windows 10 Version 1703 allows an attacker to trick a user by redirecting the user to a specially crafted website, due to the way that Microsoft Edge parses HTTP content, aka "Microsoft Edge Spoofing Vulnerability". This CVE ID is unique from CVE-2017-8735.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8729 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8731 | None | None | Microsoft Edge in Microsoft Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8734, CVE-2017-8751, and CVE-2017-11766.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8734 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8731, CVE-2017-8751, and CVE-2017-11766.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8735 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user by redirecting the user to a specially crafted website, due to the way that Microsoft Edge parses HTTP content, aka "Microsoft Edge Spoofing Vulnerability". This CVE ID is unique from CVE-2017-8724.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8736 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to obtain specific information used in the parent domain, due to Microsoft browser parent domain verification in certain functionality, aka "Microsoft Browser Information Disclosure Vulnerability".             |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8738 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8739 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8740 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8741 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8748 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8750 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browsers access objects in memory, aka "Microsoft Browser Memory Corruption Vulnerability".  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8751 | None | None | Microsoft Edge in Microsoft Windows 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-11766.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8752 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8753 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8754 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page containing malicious content, due to the way that the Edge Content Security Policy (CSP) validates certain specially crafted documents, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-8723.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8755 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8756, and CVE-2017-11764. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8756 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-11764.                                 |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8757 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way Microsoft Edge handles objects in memory, aka "Microsoft Edge Remote Code Execution Vulnerability".  |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11792 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allow an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11793, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.        |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11794 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-8726 and CVE-2017-11803.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11796 | None | None | ChakraCore and Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821. |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11798 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11799 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11800 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.                      |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11802 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11804 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11805 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.  |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11806 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11807 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11808 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821. |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11809 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11811 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11812 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821.       |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11821 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, and CVE-2017-11812. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-8726  | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how affected Microsoft scripting engines handle objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11794 and CVE-2017-11803.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11791 | None | None | ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-11834.                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11803 | None | None | Microsoft Edge in Microsoft Windows 10 1703, 1709 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-11833 and CVE-2017-11844.  |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11827 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka "Microsoft Browser Memory Corruption Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11833 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to determine the origin of all webpages in the affected browser, due to how Microsoft Edge handles cross-origin requests, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-11803 and CVE-2017-11844.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11836 | None | None | ChakraCore, and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11837 | None | None | ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11838 | None | None | ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11839 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.   |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11840 | None | None | ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11841 | None | None | ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11843 | None | None | ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11844 | None | None | Microsoft Edge in Microsoft Windows 10 1703, 1709 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-11803 and CVE-2017-11833.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11845 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11846 | None | None | ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11858 | None | None | ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.    |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11861 | None | None | Microsoft Edge in Windows 10 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11862 | None | None | ChakraCore and Microsoft Edge in Windows 10 1709 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11863 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to trick a user into loading a page containing malicious content, due to how the Edge Content Security Policy (CSP) validates documents, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-11872 and CVE-2017-11874.  |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11866 | None | None | ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11870 | None | None | ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11871, and CVE-2017-11873.                                       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11871 | None | None | ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11873.                                       |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11872 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to force the browser to send data that would otherwise be restricted to a destination website of the attacker's choice, due to how Microsoft Edge handles redirect requests, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-11863 and CVE-2017-11874.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11873 | None | None | ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11871. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11874 | None | None | Microsoft Edge in Microsoft Windows 10 1703, 1709, Windows Server, version 1709, and ChakraCore allows an attacker to bypass Control Flow Guard (CFG) to run arbitrary code on a target system, due to how Microsoft Edge handles accessing memory in code compiled by the Edge Just-In-Time (JIT) compiler, aka "Microsoft Edge Security Feature Bypass Vulnerability". This CVE ID is unique from CVE-2017-11863 and CVE-2017-11872.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11888 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability".  |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11889 | None | None | ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11893 | None | None | ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.       |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11894 | None | None | ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11895 | None | None | ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.         |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11905 | None | None | ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11912 | None | None | ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930. |

|                |                   |                |      |      |  |
|----------------|-------------------|----------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11914 | None | None | ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11918 | None | None | ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, and CVE-2017-11930. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2017-11919 | None | None | ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016, and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-11887 and CVE-2017-11906.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0758 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0762 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0766 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the Microsoft Edge PDF Reader handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0767 | None | None | Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0780 and CVE-2018-0800.  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0768 | None | None | Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0769 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0770 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0772 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0773 | None | None | Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0774 | None | None | Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0775 | None | None | Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0776 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0777 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0778, and CVE-2018-0781. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0778 | None | None | Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0781.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0780 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0800.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0781 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0778. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0800 | None | None | Microsoft Edge in Microsoft Windows 10 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0780.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0803 | None | None | Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to access information from one domain and inject it into another domain, due to how Microsoft Edge enforces cross-domain policies, aka "Microsoft Edge Elevation of Privilege Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0763 | None | None | Microsoft Edge in Microsoft Windows 10 1703 and 1709 allows information disclosure, due to how Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0839.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0771 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows a security feature bypass, due to how Edge handles different-origin requests, aka "Microsoft Edge Security Feature Bypass".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0834 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0835 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0836 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 1703 and 1709 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0837 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0838 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0839 | None | None | Microsoft Edge in Microsoft Windows 10 1703 allows information disclosure, due to how Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0763.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0840 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0856 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 1703 and 1709 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0857 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0859 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0860 | None | None | Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0861, and CVE-2018-0866. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0861 | None | None | Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, and CVE-2018-0866. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0872 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka "Chakra Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937.              |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0873 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka "Chakra Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0872, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937.                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0874 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka "Chakra Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937.              |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0876 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0889, CVE-2018-0893, CVE-2018-0925, and CVE-2018-0935.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0879 | None | None | Microsoft Edge in Windows 10 1709 allows information disclosure, due to how Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability".   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0889 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0876, CVE-2018-0893, CVE-2018-0925, and CVE-2018-0935.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0891 | None | None | ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0939. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0893 | None | None | Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0876, CVE-2018-0889, CVE-2018-0925, and CVE-2018-0935.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0927 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure, due to how Microsoft browsers handle objects in memory, aka "Microsoft Browser Information Disclosure Vulnerability".                                   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0930 | None | None | ChakraCore and Microsoft Edge in Microsoft Windows 10 1709 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka "Chakra Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0932 | None | None | Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure, due to how Microsoft browsers handle objects in memory, aka "Microsoft Browser Information Disclosure Vulnerability". |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0939 | None | None | ChakraCore and Microsoft Edge in Windows 10 1703 and 1709 allow information disclosure, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0891.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0892 | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-0998.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0979 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0980, CVE-2018-0990, CVE-2018-0993, CVE-2018-0994, CVE-2018-0995, CVE-2018-1019.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0980 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0979, CVE-2018-0990, CVE-2018-0993, CVE-2018-0994, CVE-2018-0995, CVE-2018-1019.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0990 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0979, CVE-2018-0980, CVE-2018-0993, CVE-2018-0994, CVE-2018-0995, CVE-2018-1019.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0993 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0979, CVE-2018-0980, CVE-2018-0990, CVE-2018-0994, CVE-2018-0995, CVE-2018-1019. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0994 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0979, CVE-2018-0980, CVE-2018-0990, CVE-2018-0993, CVE-2018-0995, CVE-2018-1019. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0995 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0979, CVE-2018-0980, CVE-2018-0990, CVE-2018-0993, CVE-2018-0994, CVE-2018-1019. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0998 | None | None | An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-0892.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-1019 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0979, CVE-2018-0980, CVE-2018-0990, CVE-2018-0993, CVE-2018-0994, CVE-2018-0995. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-1023 | None | None | A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka "Microsoft Browser Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0943 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8130, CVE-2018-8133, CVE-2018-8145, CVE-2018-8177.                               |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0945 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0946, CVE-2018-0951, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137, CVE-2018-8139.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0946 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0945, CVE-2018-0951, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137, CVE-2018-8139.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0951 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137, CVE-2018-8139.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0953 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0951, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137, CVE-2018-8139.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0954 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects Internet Explorer 9, ChakraCore, Internet Explorer 11, Microsoft Edge, Internet Explorer 10. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0951, CVE-2018-0953, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137, CVE-2018-8139. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-1021 | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8123.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-1022 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0951, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137, CVE-2018-8139. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-1025 | None | None | An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory, aka "Microsoft Browser Information Disclosure Vulnerability." This affects Internet Explorer 11, Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8112 | None | None | A security feature bypass vulnerability exists when Microsoft Edge improperly handles requests of different origins, aka "Microsoft Edge Security Feature Bypass Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8123 | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-1021.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8128 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0951, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8137, CVE-2018-8139.                      |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8130 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0943, CVE-2018-8133, CVE-2018-8145, CVE-2018-8177.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8133 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0943, CVE-2018-8130, CVE-2018-8145, CVE-2018-8177.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8137 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0951, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8139.                            |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8139 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-0945, CVE-2018-0946, CVE-2018-0951, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-1022, CVE-2018-8114, CVE-2018-8122, CVE-2018-8128, CVE-2018-8137.                            |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8145 | None | None | An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the user's computer or data, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge, Internet Explorer 10. This CVE ID is unique from CVE-2018-0943, CVE-2018-8130, CVE-2018-8133, CVE-2018-8177. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8177 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore. This CVE ID is unique from CVE-2018-0943, CVE-2018-8130, CVE-2018-8133, CVE-2018-8145.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8178 | None | None | A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka "Microsoft Browser Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge.  |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8179  | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-10678 | None | None | MyBB 1.8.15, when accessed with Microsoft Edge, mishandles 'target="_blank" rel="noopener"' in A elements, which makes it easier for remote attackers to conduct redirection attacks.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-0871  | None | None | An information disclosure vulnerability exists when Edge improperly marks files, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8234.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8110  | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8111, CVE-2018-8236.                                     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8111  | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8110, CVE-2018-8236.                                     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8227  | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8229. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8229  | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8227. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8234  | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-0871.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8235  | None | None | A security feature bypass vulnerability exists when Microsoft Edge improperly handles requests of different origins, aka "Microsoft Edge Security Feature Bypass Vulnerability." This affects Microsoft Edge.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8236 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8110, CVE-2018-8111.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8125 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8262, CVE-2018-8274, CVE-2018-8275, CVE-2018-8279, CVE-2018-8301.             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8262 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8125, CVE-2018-8274, CVE-2018-8275, CVE-2018-8279, CVE-2018-8301.             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8274 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8125, CVE-2018-8262, CVE-2018-8275, CVE-2018-8279, CVE-2018-8301.             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8275 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8125, CVE-2018-8262, CVE-2018-8274, CVE-2018-8279, CVE-2018-8301. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8276 | None | None | A security feature bypass vulnerability exists in the Microsoft Chakra scripting engine that allows Control Flow Guard (CFG) to be bypassed, aka "Scripting Engine Security Feature Bypass Vulnerability." This affects Microsoft Edge, ChakraCore.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8278 | None | None | A spoofing vulnerability exists when Microsoft Edge improperly handles specific HTML content, aka "Microsoft Edge Spoofing Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8279 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8125, CVE-2018-8262, CVE-2018-8274, CVE-2018-8275, CVE-2018-8301. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8280 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8286, CVE-2018-8290, CVE-2018-8294.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8286 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8280, CVE-2018-8290, CVE-2018-8294.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8287 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge, Internet Explorer 10. This CVE ID is unique from CVE-2018-8242, CVE-2018-8283, CVE-2018-8288, CVE-2018-8291, CVE-2018-8296, CVE-2018-8298. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8288 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge. This CVE ID is unique from CVE-2018-8242, CVE-2018-8283, CVE-2018-8287, CVE-2018-8291, CVE-2018-8296, CVE-2018-8298.                       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8289 | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8297, CVE-2018-8324, CVE-2018-8325.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8290 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8280, CVE-2018-8286, CVE-2018-8294.   |

|                |                   |                |      |      |   |
|----------------|-------------------|----------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8291  | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge. This CVE ID is unique from CVE-2018-8242, CVE-2018-8283, CVE-2018-8287, CVE-2018-8288, CVE-2018-8296, CVE-2018-8298. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8294  | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8280, CVE-2018-8286, CVE-2018-8290.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8297  | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8289, CVE-2018-8324, CVE-2018-8325.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8301  | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8125, CVE-2018-8262, CVE-2018-8274, CVE-2018-8275, CVE-2018-8279.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8324  | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8289, CVE-2018-8297, CVE-2018-8325.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8325  | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8289, CVE-2018-8297, CVE-2018-8324.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-12989 | None | None | The report-viewing feature in Pearson VUE Certiport Console 8 and IQSystem 7 before 2018-06-26 mishandles child processes and consequently launches Internet Explorer or Microsoft Edge as Administrator, which allows local users to gain privileges.  |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8266 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8380, CVE-2018-8381, CVE-2018-8384.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8351 | None | None | An information disclosure vulnerability exists when affected Microsoft browsers improperly allow cross-frame interaction, aka "Microsoft Browser Information Disclosure Vulnerability." This affects Internet Explorer 11, Microsoft Edge, Internet Explorer 10.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8355 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge. This CVE ID is unique from CVE-2018-8353, CVE-2018-8359, CVE-2018-8371, CVE-2018-8372, CVE-2018-8373, CVE-2018-8385, CVE-2018-8389, CVE-2018-8390. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8357 | None | None | An elevation of privilege vulnerability exists in Microsoft browsers allowing sandbox escape, aka "Microsoft Browser Elevation of Privilege Vulnerability." This affects Internet Explorer 11, Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8358 | None | None | A security feature bypass vulnerability exists when Microsoft Edge improperly handles redirect requests, aka "Microsoft Edge Security Feature Bypass Vulnerability." This affects Microsoft Edge.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8370 | None | None | An information disclosure vulnerability exists when WebAudio Library improperly handles audio requests, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8372 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge. This CVE ID is unique from CVE-2018-8353, CVE-2018-8355, CVE-2018-8359, CVE-2018-8371, CVE-2018-8373, CVE-2018-8385, CVE-2018-8389, CVE-2018-8390. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8377 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8387.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8380 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8266, CVE-2018-8381, CVE-2018-8384.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8381 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8266, CVE-2018-8380, CVE-2018-8384.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8383 | None | None | A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content, aka "Microsoft Edge Spoofing Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8388.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8384 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects ChakraCore. This CVE ID is unique from CVE-2018-8266, CVE-2018-8380, CVE-2018-8381.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8385 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects Internet Explorer 9, ChakraCore, Internet Explorer 11, Microsoft Edge, Internet Explorer 10. This CVE ID is unique from CVE-2018-8353, CVE-2018-8355, CVE-2018-8359, CVE-2018-8371, CVE-2018-8372, CVE-2018-8373, CVE-2018-8389, CVE-2018-8390. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8387 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8377.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8388 | None | None | A spoofing vulnerability exists when Microsoft Edge improperly handles specific HTML content, aka "Microsoft Edge Spoofing Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8383.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8390 | None | None | A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8353, CVE-2018-8355, CVE-2018-8359, CVE-2018-8371, CVE-2018-8372, CVE-2018-8373, CVE-2018-8385, CVE-2018-8389. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8403 | None | None | A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka "Microsoft Browser Memory Corruption Vulnerability." This affects Internet Explorer 11, Microsoft Edge, Internet Explorer 10.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8315 | None | None | An information disclosure vulnerability exists when the browser scripting engine improperly handle object types, aka "Microsoft Scripting Engine Information Disclosure Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge, Internet Explorer 10.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8354 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8391, CVE-2018-8456, CVE-2018-8457, CVE-2018-8459.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8366 | None | None | An information disclosure vulnerability exists when the Microsoft Edge Fetch API incorrectly handles a filtered response type, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8367 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8465, CVE-2018-8466, CVE-2018-8467.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8425 | None | None | A spoofing vulnerability exists when Microsoft Edge improperly handles specific HTML content, aka "Microsoft Edge Spoofing Vulnerability." This affects Microsoft Edge.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8452 | None | None | An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft browsers, aka "Scripting Engine Information Disclosure Vulnerability." This affects ChakraCore, Internet Explorer 11, Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8456 | None | None | A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8354, CVE-2018-8391, CVE-2018-8457, CVE-2018-8459.                                       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8457 | None | None | A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability." This affects Internet Explorer 11, Microsoft Edge, Internet Explorer 10. This CVE ID is unique from CVE-2018-8354, CVE-2018-8391, CVE-2018-8456, CVE-2018-8459. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8459 | None | None | A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8354, CVE-2018-8391, CVE-2018-8456, CVE-2018-8457.                                       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8463 | None | None | An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8469.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8464 | None | None | An remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka "Microsoft Edge PDF Remote Code Execution Vulnerability." This affects Microsoft Edge.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8465 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8367, CVE-2018-8466, CVE-2018-8467.                                 |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8466 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8367, CVE-2018-8465, CVE-2018-8467.                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8467 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8367, CVE-2018-8465, CVE-2018-8466.                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8469 | None | None | An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8463.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8473 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8509.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8503 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8505, CVE-2018-8510, CVE-2018-8511, CVE-2018-8513. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8505 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8503, CVE-2018-8510, CVE-2018-8511, CVE-2018-8513. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8509 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8473.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8510 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8503, CVE-2018-8505, CVE-2018-8511, CVE-2018-8513.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8511 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8503, CVE-2018-8505, CVE-2018-8510, CVE-2018-8513.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8512 | None | None | A security feature bypass vulnerability exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka "Microsoft Edge Security Feature Bypass Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8530.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8513 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8503, CVE-2018-8505, CVE-2018-8510, CVE-2018-8511.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8530 | None | None | A security feature bypass vulnerability exists when Microsoft Edge improperly handles requests of different origins, aka "Microsoft Edge Security Feature Bypass Vulnerability." This affects Microsoft Edge. This CVE ID is unique from CVE-2018-8512.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8541 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8542, CVE-2018-8543, CVE-2018-8551, CVE-2018-8555, CVE-2018-8556, CVE-2018-8557, CVE-2018-8588. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8542 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8543, CVE-2018-8551, CVE-2018-8555, CVE-2018-8556, CVE-2018-8557, CVE-2018-8588. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8543 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8542, CVE-2018-8551, CVE-2018-8555, CVE-2018-8556, CVE-2018-8557, CVE-2018-8588. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8545 | None | None | An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka "Microsoft Edge Information Disclosure Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8551 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8542, CVE-2018-8543, CVE-2018-8555, CVE-2018-8556, CVE-2018-8557, CVE-2018-8588. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8555 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8542, CVE-2018-8543, CVE-2018-8551, CVE-2018-8556, CVE-2018-8557, CVE-2018-8588. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8556 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8542, CVE-2018-8543, CVE-2018-8551, CVE-2018-8555, CVE-2018-8557, CVE-2018-8588. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8557 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8542, CVE-2018-8543, CVE-2018-8551, CVE-2018-8555, CVE-2018-8556, CVE-2018-8588. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8564 | None | None | A spoofing vulnerability exists when Microsoft Edge improperly handles specific HTML content, aka "Microsoft Edge Spoofing Vulnerability." This affects Microsoft Edge.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8567 | None | None | An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8588 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8541, CVE-2018-8542, CVE-2018-8543, CVE-2018-8551, CVE-2018-8555, CVE-2018-8556, CVE-2018-8557. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8583 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8617 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8618 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8624, CVE-2018-8629.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8624 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8629.  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2018-8629 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8624.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0539 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0567, CVE-2019-0568.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0565 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0566 | None | None | An elevation of privilege vulnerability exists in Microsoft Edge Browser Broker COM object, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0567 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0568.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0568 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0567.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-6251 | None | None | WebKitGTK and WPE WebKit prior to version 2.24.1 are vulnerable to address bar spoofing upon certain JavaScript redirections. An attacker could cause malicious web content to be displayed as if for a trusted URI. This is similar to the CVE-2018-8383 issue in Microsoft Edge.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0590 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0591 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0593 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0605 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0607 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0610 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0634 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0645, CVE-2019-0650.   |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0640 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0641 | None | None | A security feature bypass vulnerability exists in Microsoft Edge handles whitelisting, aka 'Microsoft Edge Security Feature Bypass Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0642 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0643 | None | None | An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0644 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0645 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0650.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0650 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0645.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0651 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0652, CVE-2019-0655. |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0652 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0655.                       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0655 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652.                       |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0658 | None | None | An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0648.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0592 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0611.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0611 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0592.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0612 | None | None | A security feature bypass vulnerability exists when Click2Play protection in Microsoft Edge improperly handles flash objects. By itself, this bypass vulnerability does not allow arbitrary code execution, aka 'Microsoft Edge Security Feature Bypass Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0678 | None | None | An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0746 | None | None | An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'.  |

|                |                   |               |      |      |  |
|----------------|-------------------|---------------|------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0769 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0770 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0771 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0773, CVE-2019-0783. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0773 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0783. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0779 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0739 | None | None | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0752, CVE-2019-0753, CVE-2019-0862.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0806 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861.                 |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0810 | HIGH | 7.5  | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0812 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0829 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0860, CVE-2019-0861.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0833 | None | None | An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka 'Microsoft Edge Information Disclosure Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0860 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0861.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0861 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0912 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0913 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0914 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0915 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0916 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0917 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0922 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0923 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0924 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0925 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0926 | None | None | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0927 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0933, CVE-2019-0937. |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0933 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0937. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0937 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0938 | None | None | An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, aka 'Microsoft Edge Elevation of Privilege Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-7090 | None | None | Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0989 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0990 | None | None | An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1023.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0991 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0992 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-0993 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1002 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1003 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1023 | None | None | An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0990.   |

|                |                   |               |      |      |   |
|----------------|-------------------|---------------|------|------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1024 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1051, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1051 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1052. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1052 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1062 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1092, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1092 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1103 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1106, CVE-2019-1107.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1106 | None | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1107.   |

|                |                   |               |        |      |  |
|----------------|-------------------|---------------|--------|------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1107 | None   | None | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1106.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1030 | MEDIUM | 4.3  | An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The update addresses the vulnerability by modifying how Microsoft Edge based on Edge HTML handles objects in memory.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1131 | MEDIUM | 4.2  | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |

|                |                   |               |        |     |  |
|----------------|-------------------|---------------|--------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1139 | MEDIUM | 4.2 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1140 | HIGH   | 8.8 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |

|                |                   |               |        |     |  |
|----------------|-------------------|---------------|--------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1141 | MEDIUM | 4.2 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1195 | MEDIUM | 4.2 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |

|                |                   |               |        |     |  |
|----------------|-------------------|---------------|--------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1196 | MEDIUM | 4.2 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1197 | MEDIUM | 4.2 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided co... |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1138 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1217, CVE-2019-1237, CVE-2019-1298, CVE-2019-1300.  |

|                |                   |               |        |     |   |
|----------------|-------------------|---------------|--------|-----|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1217 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1237, CVE-2019-1298, CVE-2019-1300. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1237 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1298, CVE-2019-1300. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1298 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1237, CVE-2019-1300. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1299 | MEDIUM | 6.5 | An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based on Edge HTML Information Disclosure Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1300 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1237, CVE-2019-1298. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1307 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1308 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1335 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.                |

|                |                   |                |        |     |   |
|----------------|-------------------|----------------|--------|-----|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1356  | MEDIUM | 6.5 | An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based on Edge HTML Information Disclosure Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1366  | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1413  | MEDIUM | 4.3 | A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_urls, aka 'Microsoft Edge Security Feature Bypass Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1426  | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1427, CVE-2019-1428, CVE-2019-1429.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1427  | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1428, CVE-2019-1429.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-1428  | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1429.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2019-18652 | MEDIUM | 6.1 | A DOM based XSS vulnerability has been identified on the WatchGuard XMT515 through 12.1.3, allowing a remote attacker to execute JavaScript in the victim's browser by tricking the victim into clicking on a crafted link. The payload was tested in Microsoft Internet Explorer 11.418.18362.0 and Microsoft Edge 44.18362.387.0 (Microsoft EdgeHTML 18.18362). |

|                |                   |               |        |     |  |
|----------------|-------------------|---------------|--------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-0663 | MEDIUM | 4.2 | An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-0811 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0812.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-0812 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0811.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-0816 | HIGH   | 8.8 | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-0969 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1037 | HIGH   | 7.5 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1056 | HIGH   | 8.1 | An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1059 | MEDIUM | 4.3 | A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content, aka 'Microsoft Edge Spoofing Vulnerability'.   |

|                |                   |               |          |     |  |
|----------------|-------------------|---------------|----------|-----|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1096 | HIGH     | 7.5 | A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1195 | MEDIUM   | 5.9 | An elevation of privilege vulnerability exists in Microsoft Edge (Chromium-based) when the Feedback extension improperly validates input, aka 'Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1242 | MEDIUM   | 5.3 | An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-9633 | CRITICAL | 9.8 | Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1433 | MEDIUM   | 6.5 | An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Information Disclosure Vulnerability'.   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1462 | MEDIUM   | 4.3 | An information disclosure vulnerability exists when Skype for Business is accessed via Microsoft Edge (EdgeHTML-based), aka 'Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure Vulnerability'.   |

|                |                   |               |                  |            |  |
|----------------|-------------------|---------------|------------------|------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1555 | HIGH             | 8.8        | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content o... |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1568 | ['HIGH', 'HIGH'] | [7.5, 7.5] | A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that contains malicious PDF content. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted PDF content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-cont... |

|                |                   |                |                      |            |  |
|----------------|-------------------|----------------|----------------------|------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-1569  | ['HIGH', 'HIGH']     | [7.8, 7.5] | A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability. In all cases, however, an att...     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-0908  | ['HIGH', 'HIGH']     | [7.5, 7.5] | <p>A remote code execution vulnerability exists when the Windows Text Service Module improperly handles memory. An attacker who successfully exploited the vulnerability could gain execution on a victim system.</p> <p>An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (Chromium-based), and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email.</p> <p>The security update addresses the vulnerability by correcting how the ...</p> |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2020-17153 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.1] | Microsoft Edge for Android Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-1705  | ['MEDIUM', 'HIGH']   | [4.2, 7.5] | Microsoft Edge (HTML-based) Memory Corruption Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-24100 | ['MEDIUM', 'MEDIUM'] | [5.0, 4.4] | Microsoft Edge for Android Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-24113 | ['MEDIUM', 'MEDIUM'] | [5.4, 5.4] | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability  |

|                |                   |                |                      |            |  |
|----------------|-------------------|----------------|----------------------|------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-33741 | ['HIGH', 'HIGH']     | [8.2, 7.5] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-36928 | ['MEDIUM', 'HIGH']   | [6.0, 7.8] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-36929 | ['MEDIUM', 'MEDIUM'] | [6.3, 5.5] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-36931 | ['MEDIUM', 'HIGH']   | [4.4, 7.8] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-26436 | ['MEDIUM', 'HIGH']   | [6.1, 8.1] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-26439 | ['MEDIUM', 'MEDIUM'] | [4.6, 5.9] | Microsoft Edge for Android Information Disclosure Vulnerability      |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-36930 | ['MEDIUM', 'HIGH']   | [5.3, 8.1] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-38641 | ['MEDIUM', 'MEDIUM'] | [6.1, 4.2] | Microsoft Edge for Android Spoofing Vulnerability                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-38642 | ['MEDIUM', 'MEDIUM'] | [6.1, 4.2] | Microsoft Edge for iOS Spoofing Vulnerability                        |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-38669 | ['MEDIUM', 'HIGH']   | [6.4, 8.8] | Microsoft Edge (Chromium-based) Tampering Vulnerability              |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-41351 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Microsoft Edge (Chrome based) Spoofing on IE Mode                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-42308 | ['LOW', 'HIGH']      | [3.1, 7.5] | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-43220 | ['LOW', 'HIGH']      | [3.1, 7.5] | Microsoft Edge for iOS Spoofing Vulnerability                        |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-43221 | ['MEDIUM', 'MEDIUM'] | [4.2, 4.2] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-21929 | LOW                  | 2.5        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-21930 | MEDIUM               | 4.2        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-21931 | MEDIUM               | 4.2        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-21954 | MEDIUM               | 6.1        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-21970 | ['MEDIUM', 'HIGH']   | [6.1, 7.8] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-23258 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Microsoft Edge for Android Spoofing Vulnerability                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-23261 | MEDIUM               | 5.3        | Microsoft Edge (Chromium-based) Tampering Vulnerability              |

|                |                   |                |                  |            |  |
|----------------|-------------------|----------------|------------------|------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-23262 | MEDIUM           | 6.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-23263 | HIGH             | 7.7        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-24475 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-24523 | MEDIUM           | 4.3        | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26891 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26894 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26895 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26900 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26908 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26909 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26912 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26905 | MEDIUM           | 4.3        | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-30127 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-30128 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-22021 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-30192 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-33638 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-33639 | ['HIGH', 'HIGH'] | [8.3, 8.3] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-33680 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-33636 | HIGH             | 8.3        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |

|                |                   |                |                          |            |   |
|----------------|-------------------|----------------|--------------------------|------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-33649 | ['CRITICAL', 'CRITICAL'] | [9.6, 9.6] | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-35796 | HIGH                     | 7.5        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-38012 | ['HIGH', 'HIGH']         | [7.7, 7.7] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-37968 | CRITICAL                 | 10.0       | Microsoft has identified a vulnerability affecting the cluster connect feature of Azure Arc-enabled Kubernetes clusters. This vulnerability could allow an unauthenticated user to elevate their privileges and potentially gain administrative control over the Kubernetes cluster. Additionally, because Azure Stack Edge allows customers to deploy Kubernetes workloads on their devices via Azure Arc, Azure Stack Edge devices are also vulnerable to this vulnerability. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-41035 | ['MEDIUM', 'MEDIUM']     | [5.3, 5.3] | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-41115 | ['MEDIUM', 'MEDIUM']     | [6.6, 6.6] | Microsoft Edge (Chromium-based) Update Elevation of Privilege Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-44688 | MEDIUM                   | 4.3        | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-44708 | ['HIGH', 'HIGH']         | [8.3, 8.3] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-21719 | ['MEDIUM', 'MEDIUM']     | [6.5, 6.5] | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-21775 | HIGH                     | 8.3        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-21795 | HIGH                     | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-21796 | HIGH                     | 8.3        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-21720 | MEDIUM                   | 5.3        | Microsoft Edge (Chromium-based) Tampering Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-21794 | MEDIUM                   | 4.3        | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-23374 | HIGH                     | 8.3        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-24892 | ['HIGH', 'HIGH']         | [8.2, 8.2] | Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability   |

|                |                   |                |                         |               |   |
|----------------|-------------------|----------------|-------------------------|---------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-22880 | ['MEDIUM',<br>'HIGH']   | [6.8,<br>7.5] | Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-24935 | ['MEDIUM',<br>'MEDIUM'] | [6.1,<br>6.1] | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-28284 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-28301 | ['LOW', '<br>LOW']      | [3.7,<br>3.7] | Microsoft Edge (Chromium-based) Tampering Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-28261 | ['MEDIUM',<br>'MEDIUM'] | [5.7,<br>5.7] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-28286 | MEDIUM                  | 6.1           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-29334 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-29350 | HIGH                    | 7.5           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-29354 | MEDIUM                  | 4.7           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-33143 | ['HIGH', '<br>HIGH']    | [7.5,<br>7.5] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-29345 | MEDIUM                  | 6.1           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-33145 | MEDIUM                  | 6.5           | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-31937 | HIGH                    | 8.2           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-29144 | ['HIGH', '<br>HIGH']    | [7.5,<br>7.5] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-29146 | ['HIGH', '<br>HIGH']    | [8.3,<br>8.3] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-29147 | LOW                     | 3.1           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |

|                |                   |                |                         |               |   |
|----------------|-------------------|----------------|-------------------------|---------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-26899 | ['MEDIUM',<br>'HIGH']   | [6.3,<br>8.8] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2022-23264 | MEDIUM                  | 4.7           | Microsoft Edge (Chromium-based) Spoofing Vulnerability                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-31982 | ['HIGH', '<br>HIGH']    | [8.8,<br>8.8] | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-34475 | ['MEDIUM',<br>'MEDIUM'] | [5.4,<br>5.4] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-34506 | ['MEDIUM',<br>'MEDIUM'] | [6.1,<br>6.1] | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2021-42307 | ['MEDIUM',<br>'MEDIUM'] | [4.3,<br>4.3] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36883 | MEDIUM                  | 4.3           | Microsoft Edge for iOS Spoofing Vulnerability                         |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36887 | HIGH                    | 7.8           | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36888 | MEDIUM                  | 6.3           | Microsoft Edge for Android (Chromium-based) Tampering Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-35392 | MEDIUM                  | 4.7           | Microsoft Edge (Chromium-based) Spoofing Vulnerability                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-38173 | MEDIUM                  | 4.3           | Microsoft Edge for Android Spoofing Vulnerability                     |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-38187 | MEDIUM                  | 6.5           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-38157 | MEDIUM                  | 6.5           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36787 | HIGH                    | 8.8           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-38158 | LOW                     | 3.1           | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36741 | ['HIGH', '<br>HIGH']    | [8.3,<br>7.5] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36562 | HIGH                    | 7.1           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36727 | MEDIUM                  | 6.1           | Microsoft Edge (Chromium-based) Spoofing Vulnerability                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36735 | CRITICAL                | 9.6           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36559 | MEDIUM                  | 4.2           | Microsoft Edge (Chromium-based) Spoofing Vulnerability                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36022 | ['MEDIUM',<br>'MEDIUM'] | [6.6,<br>6.6] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |

|                |                   |                |                         |               |   |
|----------------|-------------------|----------------|-------------------------|---------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36029 | ['MEDIUM',<br>'MEDIUM'] | [4.3,<br>4.3] | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36034 | ['HIGH', '<br>HIGH']    | [7.3,<br>7.3] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36409 | ['MEDIUM',<br>'MEDIUM'] | [6.5,<br>6.5] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36014 | ['HIGH', '<br>HIGH']    | [7.3,<br>7.3] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36024 | ['HIGH', '<br>HIGH']    | [7.1,<br>7.1] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36027 | ['HIGH', '<br>MEDIUM']  | [7.1,<br>6.3] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36008 | ['MEDIUM',<br>'MEDIUM'] | [6.6,<br>6.6] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36026 | ['MEDIUM',<br>'MEDIUM'] | [4.3,<br>4.3] | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-35618 | CRITICAL                | 9.6           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36880 | MEDIUM                  | 4.8           | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-38174 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2023-36878 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-22125 | ['HIGH', '<br>HIGH']    | [7.4,<br>7.5] | Under certain conditions the Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge) - version 1.0, allows an attacker to access highly sensitive information which would otherwise be restricted causing high impact on confidentiality. |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-20675 | MEDIUM                  | 6.3           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21337 | MEDIUM                  | 5.2           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21326 | CRITICAL                | 9.6           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21382 | MEDIUM                  | 4.3           | Microsoft Edge for Android Information Disclosure Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21383 | LOW                     | 3.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21385 | HIGH                    | 8.3           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |

|                |                   |                |                      |            |  |
|----------------|-------------------|----------------|----------------------|------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21387 | MEDIUM               | 5.3        | Microsoft Edge for Android Spoofing Vulnerability                                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21336 | LOW                  | 2.5        | Microsoft Edge (Chromium-based) Spoofing Vulnerability                           |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21388 | MEDIUM               | 6.5        | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21399 | HIGH                 | 8.3        | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability              |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-21423 | MEDIUM               | 4.8        | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26188 | MEDIUM               | 4.3        | Microsoft Edge (Chromium-based) Spoofing Vulnerability                           |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26192 | HIGH                 | 8.2        | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26167 | MEDIUM               | 4.3        | Microsoft Edge for Android Spoofing Vulnerability                                |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26163 | MEDIUM               | 4.7        | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability            |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26246 | ['LOW', 'LOW']       | [3.9, 3.9] | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability            |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26196 | MEDIUM               | 4.3        | Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-26247 | MEDIUM               | 4.7        | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability            |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-29057 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Microsoft Edge (Chromium-based) Spoofing Vulnerability                           |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-29049 | ['MEDIUM', 'MEDIUM'] | [4.1, 4.7] | Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability                  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-29981 | MEDIUM               | 4.3        | Microsoft Edge (Chromium-based) Spoofing Vulnerability                           |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-29986 | MEDIUM               | 5.4        | Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-29987 | MEDIUM               | 6.5        | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-29991 | MEDIUM               | 5.0        | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability            |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-30055 | MEDIUM               | 5.4        | Microsoft Edge (Chromium-based) Spoofing Vulnerability                           |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-30056 | ['HIGH', 'MEDIUM']   | [7.1, 5.4] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability             |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-30057 | MEDIUM               | 5.4        | Microsoft Edge for iOS Spoofing Vulnerability                                    |

|                |                   |                |                           |               |  |
|----------------|-------------------|----------------|---------------------------|---------------|--|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-30058 | MEDIUM                    | 5.4           | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38083 | MEDIUM                    | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38082 | MEDIUM                    | 4.7           | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38093 | MEDIUM                    | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38156 | MEDIUM                    | 6.1           | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38103 | ['MEDIUM',<br>'MEDIUM']   | [5.9,<br>5.9] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38218 | ['HIGH', '<br>HIGH']      | [8.4,<br>7.8] | Microsoft Edge (HTML-based) Memory Corruption Vulnerability          |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38219 | ['MEDIUM',<br>'CRITICAL'] | [6.5,<br>9.0] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43472 | ['MEDIUM',<br>'HIGH']     | [5.8,<br>8.3] | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38208 | MEDIUM                    | 6.1           | Microsoft Edge for Android Spoofing Vulnerability                    |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38209 | HIGH                      | 7.8           | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38210 | HIGH                      | 7.8           | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38207 | ['MEDIUM',<br>'MEDIUM']   | [6.3,<br>6.3] | Microsoft Edge (HTML-based) Memory Corruption Vulnerability          |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38222 | ['MEDIUM',<br>'MEDIUM']   | [6.5,<br>6.5] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-38221 | MEDIUM                    | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability               |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43489 | ['MEDIUM',<br>'HIGH']     | [6.5,<br>8.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43496 | ['MEDIUM',<br>'HIGH']     | [6.5,<br>8.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43566 | ['HIGH', '<br>CRITICAL']  | [7.5,<br>9.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43578 | ['HIGH', '<br>HIGH']      | [7.6,<br>8.3] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43579 | ['HIGH', '<br>HIGH']      | [7.6,<br>8.3] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability  |

|                |                   |                |                         |               |   |
|----------------|-------------------|----------------|-------------------------|---------------|---|
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43580 | MEDIUM                  | 5.4           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43587 | ['MEDIUM',<br>'HIGH']   | [5.9,<br>8.1] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43595 | ['MEDIUM',<br>'HIGH']   | [6.5,<br>8.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43596 | ['MEDIUM',<br>'HIGH']   | [6.5,<br>8.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-49023 | ['MEDIUM',<br>'MEDIUM'] | [5.9,<br>5.3] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-43577 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-49025 | ['MEDIUM',<br>'MEDIUM'] | [5.4,<br>4.3] | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-49054 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2024-49041 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21185 | MEDIUM                  | 6.5           | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21399 | HIGH                    | 7.4           | Microsoft Edge (Chromium-based) Update Elevation of Privilege Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21262 | ['MEDIUM',<br>'MEDIUM'] | [5.4,<br>5.4] | User Interface (UI) Misrepresentation of Critical Information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21253 | MEDIUM                  | 5.3           | Microsoft Edge for IOS and Android Spoofing Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21267 | MEDIUM                  | 4.4           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21279 | ['MEDIUM',<br>'HIGH']   | [6.5,<br>8.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21283 | ['MEDIUM',<br>'HIGH']   | [6.5,<br>8.8] | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21342 | HIGH                    | 8.8           | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21404 | MEDIUM                  | 4.3           | Microsoft Edge (Chromium-based) Spoofing Vulnerability  |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21408 | HIGH                    | 8.8           | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability   |
| Microsoft Edge | 136.0.324<br>0.50 | CVE-2025-21401 | MEDIUM                  | 4.5           | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability   |

|                                    |                   |                |                         |               |   |
|------------------------------------|-------------------|----------------|-------------------------|---------------|---|
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-26643 | ['MEDIUM',<br>'MEDIUM'] | [5.4,<br>5.4] | The UI performs the wrong action in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.   |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-29795 | HIGH                    | 7.8           | Improper link resolution before file access ('link following') in Microsoft Edge (Chromium-based) allows an authorized attacker to elevate privileges locally.  |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-29806 | ['MEDIUM',<br>'MEDIUM'] | [6.5,<br>6.5] | No cwe for this issue in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.  |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-25000 | HIGH                    | 8.8           | Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.  |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-25001 | MEDIUM                  | 4.3           | Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.   |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-29796 | MEDIUM                  | 4.7           | User interface (ui) misrepresentation of critical information in Microsoft Edge for iOS allows an unauthorized attacker to perform spoofing over a network.   |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-29815 | HIGH                    | 7.6           | Use after free in Microsoft Edge (Chromium-based) allows an authorized attacker to execute code over a network.   |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-29834 | HIGH                    | 7.5           | Out-of-bounds read in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.   |
| Microsoft Edge                     | 136.0.324<br>0.50 | CVE-2025-29825 | MEDIUM                  | 6.5           | User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.  |
| Microsoft Edge<br>WebView2 Runtime | 136.0.324<br>0.50 | CVE-2023-22880 | ['MEDIUM',<br>'HIGH']   | [6.8,<br>7.5] | Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior. |

|                    |                      |                |                         |               |  |
|--------------------|----------------------|----------------|-------------------------|---------------|--|
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2018-0592  | None                    | None          | Untrusted search path vulnerability in Microsoft OneDrive allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.  |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2018-0593  | None                    | None          | Untrusted search path vulnerability in the installer of Microsoft OneDrive allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.   |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2020-0654  | CRITICAL                | 9.1           | A security feature bypass vulnerability exists in Microsoft OneDrive App for Android. This could allow an attacker to bypass the passcode or fingerprint requirements of the App. The security update addresses the vulnerability by correcting the way Microsoft OneDrive App for Android handles sharing links., aka 'Microsoft OneDrive for Android Security Feature Bypass Vulnerability'.   |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2020-1465  | HIGH                    | 7.8           | An elevation of privilege vulnerability exists in Microsoft OneDrive that allows file deletion in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft OneDrive Elevation of Privilege Vulnerability'.  |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2022-23255 | ['MEDIUM',<br>'MEDIUM'] | [5.9,<br>6.8] | Microsoft OneDrive for Android Security Feature Bypass Vulnerability   |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2023-24882 | MEDIUM                  | 5.5           | Microsoft OneDrive for Android Information Disclosure Vulnerability  |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2023-24890 | MEDIUM                  | 6.5           | Microsoft OneDrive for iOS Security Feature Bypass Vulnerability   |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2023-24923 | MEDIUM                  | 5.5           | Microsoft OneDrive for Android Information Disclosure Vulnerability  |
| Microsoft OneDrive | 25.065.04<br>06.0002 | CVE-2023-24930 | HIGH                    | 7.8           | Microsoft OneDrive for MacOS Elevation of Privilege Vulnerability  |
| MySQL Server 8.0   | 8.0.36               | CVE-2006-2042  | None                    | None          | Adobe Dreamweaver 8 before 8.0.2 and MX 2004 can generate code that allows SQL injection attacks in the (1) ColdFusion, (2) PHP mySQL, (3) ASP, (4) ASP.NET, and (5) JSP server models.  |
| MySQL Server 8.0   | 8.0.36               | CVE-2016-6663  | None                    | None          | Race condition in Oracle MySQL before 5.5.52, 5.6.x before 5.6.33, 5.7.x before 5.7.15, and 8.x before 8.0.1; MariaDB before 5.5.52, 10.0.x before 10.0.28, and 10.1.x before 10.1.18; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17 allows local users with certain permissions to gain privileges by leveraging use of my_copystat by REPAIR TABLE to repair a MyISAM table. |

|                  |        |               |        |      |   |
|------------------|--------|---------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3054 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3056 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3060 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). |

|                  |        |               |      |      |  |
|------------------|--------|---------------|------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3062 | None | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via memcached to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3064 | HIGH | 7.1  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3065 | None | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3067 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).          |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3073 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3074 | MEDIUM | 5.3 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3075 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3077 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3078 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3079 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3080 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3082 | LOW    | 2.7 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3084 | LOW    | 2.8 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell: Core / Client). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 2.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3133 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3137 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3143 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3144 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3145 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3155 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3156 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3161 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3162 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3170 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                  |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3171 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3173 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3174 | MEDIUM | 5.3  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H). |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3182 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3185 | MEDIUM | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3186 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3187 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3195 | MEDIUM | 5.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).                            |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3200 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3203 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3212 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3247 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3251 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3276 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3277 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                              |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3278 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: RBR). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3279 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                  |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3280 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: JSON). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3282 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3283 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Logging). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3284 | MEDIUM | 4.4  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3285 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Windows). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                        |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3286 | MEDIUM | 4.3 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).                             |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2420 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2434 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).     |

|                  |        |               |        |      |   |
|------------------|--------|---------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2436 | MEDIUM | 5.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2455 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2481 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2482 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |      |   |
|------------------|--------|---------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2486 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2494 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2495 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2502 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |      |   |
|------------------|--------|---------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2503 | MEDIUM | 6.4  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2507 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2510 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2513 | LOW    | 2.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2528 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2529 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2530 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2531 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2532 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).          |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2533 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).                        |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2534 | HIGH   | 7.1 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2535 | MEDIUM | 4.1 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2536 | MEDIUM | 5.0 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/R:S/C:C/N:I/N/A:H). |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2537 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2539 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2018-3123 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: libmysqld). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2566 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2580 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2581 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2584 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2585 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                 |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2587 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2589 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2592 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2593 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2596 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2606 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2607 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2614 | MEDIUM | 4.4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2617 | MEDIUM | 4.4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2620 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2623 | MEDIUM | 5.3 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2624 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2625 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2626 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2627 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2628 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |      |  |
|------------------|--------|---------------|--------|------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2630 | MEDIUM | 4.4  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2631 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2632 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2634 | MEDIUM | 5.1  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2635 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2636 | MEDIUM | 4.4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Protocol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2644 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2681 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).              |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2683 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2685 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2686 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2687 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                      |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2688 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2689 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2691 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2693 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).        |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2694 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2695 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2737 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2738 | LOW    | 3.1 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Compiling). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).                                |

|                  |        |               |        |      |   |
|------------------|--------|---------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2739 | MEDIUM | 5.1  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2740 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2741 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2743 | MEDIUM | 5.3 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2746 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Data Dictionary). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2747 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).              |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2752 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).          |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2755 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2757 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2758 | MEDIUM | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2774 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2778 | MEDIUM | 5.4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2780 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Components / Services). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2784 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2785 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |      |   |
|------------------|--------|---------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2789 | LOW    | 2.7  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/L/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2791 | None   | None | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2795 | MEDIUM | 6.5  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2796 | MEDIUM | 4.9  | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2797 | MEDIUM | 4.2 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2798 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2800 | HIGH   | 7.1 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2801 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2802 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2803 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2805 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2808 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                    |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2810 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2811 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2812 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2814 | LOW    | 2.2 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N).                                      |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2815 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2819 | MEDIUM | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2822 | HIGH   | 7.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell: Admin / InnoDB Cluster). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).   |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2826 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2830 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2834 | MEDIUM | 6.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2879 | MEDIUM | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2911 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2914 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2938 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2946 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                   |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2948 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2950 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                        |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2957 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2960 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2963 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2966 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2967 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2968 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2969 | MEDIUM | 6.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2974 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2982 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2991 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2993 | MEDIUM | 5.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2997 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-2998 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-3003 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                              |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2019-3004 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-3009 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection). Supported versions that are affected are 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-3011 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).         |
| MySQL Server 8.0 | 8.0.36 | CVE-2019-3018 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).             |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2572 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plugin). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).                                |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2577 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                             |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2579 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2580 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2584 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2588 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                        |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2589 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.28 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2627 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                      |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2660 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2679 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2686 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2694 | LOW    | 3.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.18 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).                                       |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2759 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2760 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2761 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2762 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2763 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2765 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2770 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2774 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                               |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2779 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2780 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2804 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).      |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2812 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2814 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.47 and prior, 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2853 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2892 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                             |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2893 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2895 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2896 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2897 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).          |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2898 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). The supported version that is affected is 8.0.19. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2901 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2903 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2904 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2921 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2923 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2924 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2925 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2926 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2928  | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-2930  | MEDIUM               | 4.4        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14539 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14540 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                        |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14547 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14553 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).                |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14559 | ['MEDIUM', 'MEDIUM'] | [4.3, 4.3] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14567 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14568 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14575 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14576 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14586 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).    |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14591 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14597 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14614 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14619 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).        |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14620 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14623 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14624 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14631 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Audit). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14632 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14633 | ['LOW', 'LOW']       | [2.7, 2.7] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).                               |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14634 | ['LOW', 'LOW']       | [2.7, 2.7] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14641 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14643 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14651 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14654 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14656 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14663 | ['HIGH', 'HIGH']     | [7.2, 7.2] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).                                |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14678 | ['HIGH', 'HIGH']     | [7.2, 7.2] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).                                |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14680 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14697 | ['HIGH', 'HIGH']     | [7.2, 7.2] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).                                |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14702 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14725 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14672 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14765 | MEDIUM               | 6.5        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).               |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14769 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14771 | LOW    | 2.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14773 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14775 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                              |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14776 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14777 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14785 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14786 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14789 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14790 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14791 | LOW    | 2.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14793 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14794 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14799 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14800 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14804 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14809 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14812 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14814 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14821 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14827 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14828 | HIGH   | 7.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14829 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14830 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                            |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14836 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14837 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14838 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14839 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14844 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14845 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14846 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14848 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14852 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14860 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14861 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14866 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14867 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14868 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14869 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14870 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                     |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14873 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                               |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14878 | HIGH   | 8.0 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14888 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                               |
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14891 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                               |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2020-14893 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-1998  | LOW    | 3.8 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2001  | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2002  | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2009 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).      |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2012 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2016 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2019 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).                            |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2020 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                                |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2021 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                               |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2022 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2024 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                                |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2028 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2030 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2031 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2032 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).       |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2036 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2038 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2042 | LOW    | 2.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2046 | MEDIUM | 6.8 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2048 | MEDIUM | 5.0 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2055 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2056 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2058 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2060 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2061 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2065 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2070 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2072 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).      |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2076 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2081 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).      |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2087 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2088 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2122 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2144 | HIGH   | 7.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2146 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2160 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2162 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2164 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2166 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2169 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2170 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2171 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2172 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                                 |

|                  |        |               |                      |            |  |
|------------------|--------|---------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2174 | MEDIUM               | 4.4        | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2178 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2179 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2180 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2193 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2194 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2196 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2201 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2202 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2203 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2208 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2212 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2213 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2215 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2217 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2226 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2230 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2232 | LOW    | 1.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2278 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2293 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2298 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2299 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2300 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2301 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).                   |

|                  |        |               |                      |            |   |
|------------------|--------|---------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2304 | MEDIUM               | 5.5        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2305 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2307 | ['MEDIUM', 'MEDIUM'] | [6.1, 6.1] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2308 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2339 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                            |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2340 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).                                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2342 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2352 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2354 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2356 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2357 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2367 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2370 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2372 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2374 | MEDIUM | 4.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).        |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2383 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2384 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2385 | MEDIUM | 5.0 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2387 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2389 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2390 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2399 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2402 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2410 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2412 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2417 | MEDIUM | 6.0 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2418 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |               |        |     |   |
|------------------|--------|---------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2422 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2424 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2425 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2426 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2427 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2429 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).          |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2437 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2440 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |

|                  |        |               |        |     |  |
|------------------|--------|---------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2441 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2444 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2478 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2479 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-2481  | MEDIUM               | 6.5        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35537 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).         |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35546 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35575 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35577 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via MySQL Protocol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).          |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35583 | ['HIGH', 'HIGH']     | [7.5, 7.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Windows). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35591 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35596 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35602 | ['MEDIUM', 'MEDIUM'] | [5.0, 5.0] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35604 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35607 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35608 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35610 | ['HIGH', 'HIGH']     | [7.1, 7.1] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35612 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35622 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35623 | LOW                  | 2.7        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35624 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35625 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35626 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35627 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35628 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35629 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35630 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35631 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35632 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35633 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).                                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35634 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35635 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                         |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35636 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35637 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35638 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35639 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35640 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).                        |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35641 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35642 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35643 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35644 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35645 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35646 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35647 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2021-35648 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21245 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21249 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).                                |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21253 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21254 | MEDIUM | 5.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21256 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21264 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21265 | LOW    | 3.8 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21270 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21278 | HIGH   | 7.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21297 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21301 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).      |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21302 | MEDIUM | 5.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21303 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21304 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21339 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                             |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21342 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21344 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21348 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21351 | HIGH   | 7.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21352 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21358 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21362 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21367 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21368 | MEDIUM | 4.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21370 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21372 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21374 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21378 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21379 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21412 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21413 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).         |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21414 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21415 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21417 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21418 | MEDIUM | 5.0 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21423 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21425 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21427 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21435 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21436 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21437 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21438 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21440 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21444 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21451 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21452 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21454 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21457 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21459 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21460 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21462 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21478 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21479 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H).                  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21455 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21509 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21515 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.38 and prior and 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21517 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21522 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.29 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21525 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21526 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21527 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21528 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21529 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21530 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21531 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21534 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21537 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21538 | LOW    | 3.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.29 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21539 | MEDIUM | 5.0 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21547 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21553 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21556 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21569 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21589 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.39 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21592 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.39 and prior and 8.0.29 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21594 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21595 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21599 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21600 | HIGH   | 7.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21604 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21605 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21607 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21608 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21611 | MEDIUM | 4.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21617 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.39 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21625 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21632 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21633 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21635 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21637 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21638 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21640 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-21641 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2022-39400 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-39408 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2022-39410 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21836 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21863 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21864 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21865 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21866 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21867 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21868 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21869 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21870 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21871 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21872 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21873 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21874 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).   |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21875 | ['MEDIUM', 'MEDIUM'] | [5.9, 5.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21876 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21877 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21878 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21879 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21880 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21881 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21882 | ['LOW', 'LOW']       | [2.7, 2.7] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21883 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21887 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21911 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21912 | HIGH   | 7.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.41 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21913 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21917 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21919 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21920 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21929 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21933 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21935 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21940 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21945 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21946 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).              |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21947 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21953 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21955 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21962 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21963 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.40 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21966 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |

|                  |        |                |                  |            |   |
|------------------|--------|----------------|------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21972 | MEDIUM           | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21976 | MEDIUM           | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21977 | MEDIUM           | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21980 | ['HIGH', 'HIGH'] | [7.1, 7.1] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21982 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                        |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-21950 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22005 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22007 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22008 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22033 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).          |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22038 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22046 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22048 | LOW    | 3.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22053 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.42 and prior and 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22054 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22056 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22057 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22058 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22015 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22026 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22028 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.43 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22032 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22059 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22064 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22065 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22066 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22068 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22070 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22078 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).        |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22079 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22084 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.43 and prior, 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22092 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22094 | HIGH   | 7.9 | Vulnerability in the MySQL Installer product of Oracle MySQL (component: Installer: General). Supported versions that are affected are Prior to 1.6.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Installer executes to compromise MySQL Installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Installer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Installer. Note: This patch is used in MySQL Server bundled version 8.0.35 and 5.7.44. CVSS 3.1 Base Score 7.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22097 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22103 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22104 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22110 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22111 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22112 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22113 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).                                    |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22114 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2023-22115 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                          |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20961 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20963 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20965 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20967 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20969 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20971 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20973 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20977 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20981 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20983 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20985 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20960 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: RAPID). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20962 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).              |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20964 | MEDIUM | 5.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20966 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).             |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20968 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20970 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20972 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20974 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20976 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20978 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).              |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20982 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).              |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20984 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server : Security : Firewall). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20993 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).              |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20994 | MEDIUM | 5.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20998 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21000 | LOW    | 3.8 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21008 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21009 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21013 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21015 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21047 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21049 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21050 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21051 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21052 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21053 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21054 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21055 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21056 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21057 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                           |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21060 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21061 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21062 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21069 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21087 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21096 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21102 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-20996 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                 |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21125 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21127 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21129 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21130 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21134 | MEDIUM | 4.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21135 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21137 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21142 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21157 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21159 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                       |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21160 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21162 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21163 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21165 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 8.0.37 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21166 | MEDIUM | 5.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21171 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21173 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21177 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21179 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21185 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38, 8.4.1 and 9.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21193 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21194 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).     |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21196 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21197 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21198 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21199 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |

|                  |        |                |                      |            |   |
|------------------|--------|----------------|----------------------|------------|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21200 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                                      |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21201 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21203 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21207 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38 and prior, 8.4.1 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).            |

|                  |        |                |                      |            |  |
|------------------|--------|----------------|----------------------|------------|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21212 | MEDIUM               | 4.4        | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Health Monitor). Supported versions that are affected are 8.0.39 and prior and 8.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21213 | MEDIUM               | 4.2        | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21218 | MEDIUM               | 4.9        | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21219 | ['MEDIUM', 'MEDIUM'] | [4.9, 4.9] | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21230 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).     |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21231 | LOW    | 3.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).                |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21236 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21237 | LOW    | 2.2 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21238 | MEDIUM | 5.3 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.39 and prior, 8.4.1 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21239 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |
| MySQL Server 8.0 | 8.0.36 | CVE-2024-21241 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21490 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21491 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21492 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21494 | MEDIUM | 4.1 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21497 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21500 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21501 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21503 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21504 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).              |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21505 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21518 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).               |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21519 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21520 | LOW    | 1.8 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 1.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21521 | HIGH   | 7.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21522 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21523 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21525 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21529 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21531 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                     |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21534 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Performance Schema). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21536 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21540 | MEDIUM | 5.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21543 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).  |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21546 | LOW    | 3.8 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).      |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21555 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21559 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21574 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21575 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21577 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).           |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21579 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21580 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21581 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21584 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).       |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-21585 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30681 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).            |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30682 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30683 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30684 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30685 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30687 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30688 | MEDIUM | 6.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).    |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30689 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |  |
|------------------|--------|----------------|--------|-----|--|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30693 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30695 | MEDIUM | 5.5 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30696 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |

|                  |        |                |        |     |   |
|------------------|--------|----------------|--------|-----|---|
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30699 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).      |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30703 | LOW    | 2.7 | Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).   |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30704 | MEDIUM | 4.4 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). |
| MySQL Server 8.0 | 8.0.36 | CVE-2025-30705 | MEDIUM | 4.9 | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).                    |

|                  |         |                |        |      |   |
|------------------|---------|----------------|--------|------|---|
| MySQL Server 8.0 | 8.0.36  | CVE-2025-30715 | MEDIUM | 4.9  | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).   |
| MySQL Server 8.0 | 8.0.36  | CVE-2025-30721 | MEDIUM | 4.0  | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:H). |
| Node.js          | 20.17.0 | CVE-2011-5037  | None   | None | Google V8 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters, as demonstrated by attacks against Node.js.   |
| Node.js          | 20.17.0 | CVE-2012-2330  | None   | None | The Update method in src/node_http_parser.cc in Node.js before 0.6.17 and 0.7 before 0.7.8 does not properly check the length of a string, which allows remote attackers to obtain sensitive information (request header contents) and possibly spoof HTTP headers via a zero length string.  |
| Node.js          | 20.17.0 | CVE-2013-4660  | None   | None | The JS-YAML module before 2.0.5 for Node.js parses input without properly considering the unsafe !js/function tag, which allows remote attackers to execute arbitrary code via a crafted string that triggers an eval operation.  |
| Node.js          | 20.17.0 | CVE-2013-4450  | None   | None | The HTTP server in Node.js 0.10.x before 0.10.21 and 0.8.x before 0.8.26 allows remote attackers to cause a denial of service (memory and CPU consumption) by sending a large number of pipelined requests without reading the response.  |

|         |         |               |      |      |   |
|---------|---------|---------------|------|------|---|
| Node.js | 20.17.0 | CVE-2013-7379 | None | None | The admin API in the tomato module before 0.0.6 for Node.js does not properly check the access key when it is set to a string, which allows remote attackers to bypass authentication via a string in the access-key header that partially matches config.master.api.access_key.  |
| Node.js | 20.17.0 | CVE-2014-3742 | None | None | The hapi server framework 2.0.x and 2.1.x before 2.2.0 for Node.js allows remote attackers to cause a denial of service (file descriptor consumption and process crash) via unspecified vectors.  |
| Node.js | 20.17.0 | CVE-2014-5256 | None | None | Node.js 0.8 before 0.8.28 and 0.10 before 0.10.30 does not consider the possibility of recursive processing that triggers V8 garbage collection in conjunction with a V8 interrupt, which allows remote attackers to cause a denial of service (memory corruption and application crash) via deep JSON objects whose parsing lets this interrupt mask an overflow of the program stack. |
| Node.js | 20.17.0 | CVE-2014-6394 | None | None | visionmedia send before 0.8.4 for Node.js uses a partial comparison for verifying whether a directory is within the document root, which allows remote attackers to access restricted directories, as demonstrated using "public-restricted" under a "public" directory.  |
| Node.js | 20.17.0 | CVE-2014-7205 | None | None | Eval injection vulnerability in the internals.batch function in lib/batch.js in the bassmaster plugin before 1.5.2 for the hapi server framework for Node.js allows remote attackers to execute arbitrary Javascript code via unspecified vectors.  |
| Node.js | 20.17.0 | CVE-2014-7191 | None | None | The qs module before 1.0.0 in Node.js does not call the compact function for array data, which allows remote attackers to cause a denial of service (memory consumption) by using a large index value to create a sparse array.   |
| Node.js | 20.17.0 | CVE-2014-7192 | None | None | Eval injection vulnerability in index.js in the syntax-error package before 1.1.1 for Node.js 0.10.x, as used in IBM Rational Application Developer and other products, allows remote attackers to execute arbitrary code via a crafted file.   |
| Node.js | 20.17.0 | CVE-2014-7193 | None | None | The Crumb plugin before 3.0.0 for Node.js does not properly restrict token access in situations where a hapi route handler has CORS enabled, which allows remote attackers to obtain sensitive information, and potentially obtain the ability to spoof requests to non-CORS routes, via a crafted web site that is visited by an application consumer.                                 |

|         |         |               |      |      |   |
|---------|---------|---------------|------|------|---|
| Node.js | 20.17.0 | CVE-2015-1164 | None | None | Open redirect vulnerability in the serve-static plugin before 1.7.2 for Node.js, when mounted at the root, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a // (slash slash) followed by a domain in the PATH_INFO to the default URI.   |
| Node.js | 20.17.0 | CVE-2015-1369 | None | None | SQL injection vulnerability in Sequelize before 2.0.0-rc7 for Node.js allows remote attackers to execute arbitrary SQL commands via the order parameter.  |
| Node.js | 20.17.0 | CVE-2015-1370 | None | None | Incomplete blacklist vulnerability in marked 0.3.2 and earlier for Node.js allows remote attackers to conduct cross-site scripting (XSS) attacks via a vbscript tag in a link.  |
| Node.js | 20.17.0 | CVE-2014-9682 | None | None | The dns-sync module before 0.1.1 for node.js allows context-dependent attackers to execute arbitrary commands via shell metacharacters in the first argument to the resolve API function.   |
| Node.js | 20.17.0 | CVE-2015-5380 | None | None | The Utf8DecoderBase::WriteUtf16Slow function in unicode-decoder.cc in Google V8, as used in Node.js before 0.12.6, io.js before 1.8.3 and 2.x before 2.3.3, and other products, does not verify that there is memory available for a UTF-16 surrogate pair, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted byte sequence. |
| Node.js | 20.17.0 | CVE-2015-5688 | None | None | Directory traversal vulnerability in lib/app/index.js in Geddy before 13.0.8 for Node.js allows remote attackers to read arbitrary files via a ..%2f (dot dot encoded slash) in the PATH_INFO to the default URI.   |
| Node.js | 20.17.0 | CVE-2015-8027 | None | None | Node.js 0.12.x before 0.12.9, 4.x before 4.2.3, and 5.x before 5.1.1 does not ensure the availability of a parser for each HTTP socket, which allows remote attackers to cause a denial of service (uncaughtException and service outage) via a pipelined HTTP request.   |
| Node.js | 20.17.0 | CVE-2016-2537 | None | None | The is-my-json-valid package before 2.12.4 for Node.js has an incorrect exports['utc-millisec'] regular expression, which allows remote attackers to cause a denial of service (blocked event loop) via a crafted string.   |
| Node.js | 20.17.0 | CVE-2016-2086 | None | None | Node.js 0.10.x before 0.10.42, 0.12.x before 0.12.10, 4.x before 4.3.0, and 5.x before 5.6.0 allow remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header.   |

|         |         |               |      |      |  |
|---------|---------|---------------|------|------|--|
| Node.js | 20.17.0 | CVE-2016-2216 | None | None | The HTTP header parsing code in Node.js 0.10.x before 0.10.42, 0.11.6 through 0.11.16, 0.12.x before 0.12.10, 4.x before 4.3.0, and 5.x before 5.6.0 allows remote attackers to bypass an HTTP response-splitting protection mechanism via UTF-8 encoded Unicode characters in the HTTP header, as demonstrated by %c4%8d%c4%8a. |
| Node.js | 20.17.0 | CVE-2016-1202 | None | None | Untrusted search path vulnerability in Atom Electron before 0.33.5 allows local users to gain privileges via a Trojan horse Node.js module in a parent directory of a directory named on a require line.   |
| Node.js | 20.17.0 | CVE-2016-3956 | HIGH | 7.5  | The CLI in npm before 2.15.1 and 3.x before 3.8.3, as used in Node.js 0.10 before 0.10.44, 0.12 before 0.12.13, 4 before 4.4.2, and 5 before 5.10.0, includes bearer tokens with arbitrary requests, which allows remote HTTP servers to obtain sensitive information by reading Authorization headers.                          |
| Node.js | 20.17.0 | CVE-2016-7191 | None | None | The Microsoft Azure Active Directory Passport (aka Passport-Azure-AD) library 1.x before 1.4.6 and 2.x before 2.0.1 for Node.js does not recognize the validateIssuer setting, which allows remote attackers to bypass authentication via a crafted token.   |
| Node.js | 20.17.0 | CVE-2016-5325 | None | None | CRLF injection vulnerability in the ServerResponse#writeHead function in Node.js 0.10.x before 0.10.47, 0.12.x before 0.12.16, 4.x before 4.6.0, and 6.x before 6.7.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the reason argument.                              |
| Node.js | 20.17.0 | CVE-2016-7099 | None | None | The tls.checkServerIdentity function in Node.js 0.10.x before 0.10.47, 0.12.x before 0.12.16, 4.x before 4.6.0, and 6.x before 6.7.0 does not properly handle wildcards in name fields of X.509 certificates, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.                               |
| Node.js | 20.17.0 | CVE-2013-7451 | None | None | The validator module before 1.1.0 for Node.js allows remote attackers to bypass the XSS filter via a nested tag.   |
| Node.js | 20.17.0 | CVE-2013-7452 | None | None | The validator module before 1.1.0 for Node.js allows remote attackers to bypass the cross-site scripting (XSS) filter via a crafted javascript URI.  |
| Node.js | 20.17.0 | CVE-2013-7453 | None | None | The validator module before 1.1.0 for Node.js allows remote attackers to bypass the cross-site scripting (XSS) filter via vectors related to UI redressing.  |

|         |         |               |                  |            |   |
|---------|---------|---------------|------------------|------------|---|
| Node.js | 20.17.0 | CVE-2013-7454 | None             | None       | The validator module before 1.1.0 for Node.js allows remote attackers to bypass the cross-site scripting (XSS) filter via nested forbidden strings.   |
| Node.js | 20.17.0 | CVE-2014-9772 | None             | None       | The validator package before 2.0.0 for Node.js allows remote attackers to bypass the cross-site scripting (XSS) filter via hex-encoded characters.  |
| Node.js | 20.17.0 | CVE-2015-8315 | ['HIGH', 'HIGH'] | [7.5, 7.5] | The ms package before 0.7.1 for Node.js allows attackers to cause a denial of service (CPU consumption) via a long version string, aka a "regular expression denial of service (ReDoS)."  |
| Node.js | 20.17.0 | CVE-2015-8854 | HIGH             | 7.5        | The marked package before 0.3.4 for Node.js allows attackers to cause a denial of service (CPU consumption) via unspecified vectors that trigger a "catastrophic backtracking issue for the em inline rule," aka a "regular expression denial of service (ReDoS)."                      |
| Node.js | 20.17.0 | CVE-2015-8855 | None             | None       | The semver package before 4.3.2 for Node.js allows attackers to cause a denial of service (CPU consumption) via a long version string, aka a "regular expression denial of service (ReDoS)."  |
| Node.js | 20.17.0 | CVE-2015-8856 | MEDIUM           | 6.1        | Cross-site scripting (XSS) vulnerability in the serve-index package before 1.6.3 for Node.js allows remote attackers to inject arbitrary web script or HTML via a crafted file or directory name.   |
| Node.js | 20.17.0 | CVE-2015-8857 | CRITICAL         | 9.8        | The uglify-js package before 2.4.24 for Node.js does not properly account for non-boolean values when rewriting boolean expressions, which might allow attackers to bypass security mechanisms or possibly have unspecified other impact by leveraging improperly rewritten Javascript. |
| Node.js | 20.17.0 | CVE-2015-8858 | None             | None       | The uglify-js package before 2.6.0 for Node.js allows attackers to cause a denial of service (CPU consumption) via crafted input in a parse call, aka a "regular expression denial of service (ReDoS)."   |
| Node.js | 20.17.0 | CVE-2015-8859 | MEDIUM           | 5.3        | The send package before 0.11.1 for Node.js allows attackers to obtain the root path via unspecified vectors.  |
| Node.js | 20.17.0 | CVE-2015-8860 | None             | None       | The tar package before 2.0.0 for Node.js allows remote attackers to write to arbitrary files via a symlink attack in an archive.  |
| Node.js | 20.17.0 | CVE-2015-8861 | MEDIUM           | 6.1        | The handlebars package before 4.0.0 for Node.js allows remote attackers to conduct cross-site scripting (XSS) attacks by leveraging a template with an attribute that is not quoted.  |

|         |         |                |          |      |  |
|---------|---------|----------------|----------|------|--|
| Node.js | 20.17.0 | CVE-2015-8862  | None     | None | mustache package before 2.2.1 for Node.js allows remote attackers to conduct cross-site scripting (XSS) attacks by leveraging a template with an attribute that is not quoted.   |
| Node.js | 20.17.0 | CVE-2016-4055  | MEDIUM   | 6.5  | The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)."  |
| Node.js | 20.17.0 | CVE-2017-5941  | CRITICAL | 9.8  | An issue was discovered in the node-serialize package 0.0.4 for Node.js. Untrusted data passed into the unserialize() function can be exploited to achieve arbitrary code execution by passing a JavaScript Object with an Immediately Invoked Function Expression (IIFE).   |
| Node.js | 20.17.0 | CVE-2017-5954  | None     | None | An issue was discovered in the serialize-to-js package 0.5.0 for Node.js. Untrusted data passed into the deserialize() function can be exploited to achieve arbitrary code execution by passing a JavaScript Object with an Immediately Invoked Function Expression (IIFE).  |
| Node.js | 20.17.0 | CVE-2017-7474  | None     | None | It was found that the Keycloak Node.js adapter 2.5 - 3.0 did not handle invalid tokens correctly. An attacker could use this flaw to bypass authentication and gain access to restricted information, or to possibly conduct further attacks.  |
| Node.js | 20.17.0 | CVE-2017-11499 | None     | None | Node.js v4.0 through v4.8.3, all versions of v5.x, v6.0 through v6.11.0, v7.0 through v7.10.0, and v8.0 through v8.1.3 was susceptible to hash flooding remote DoS attacks as the HashTable seed was constant across a given released version of Node.js. This was a result of building with V8 snapshots enabled by default which caused the initially randomized seed to be overwritten on startup.  |
| Node.js | 20.17.0 | CVE-2017-12581 | None     | None | GitHub Electron before 1.6.8 allows remote command execution because of a nodeIntegration bypass vulnerability. This also affects all applications that bundle Electron code equivalent to 1.6.8 or earlier. Bypassing the Same Origin Policy (SOP) is a precondition; however, recent Electron versions do not have strict SOP enforcement. Combining an SOP bypass with a privileged URL internally used by Electron, it was possible to execute native Node.js primitives in order to run OS commands on the user's host. Specifically, a chrome-devtools://devtools/bundled/inspector.html window could be used to eval a Node.js child_process.execFile API call. |

|         |         |                      |          |      |  |
|---------|---------|----------------------|----------|------|--|
| Node.js | 20.17.0 | CVE-2014-6393        | None     | None | The Express web framework before 3.11 and 4.x before 4.5 for Node.js does not provide a charset field in HTTP Content-Type headers in 400 level responses, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via characters in a non-standard encoding.                       |
| Node.js | 20.17.0 | CVE-2017-14849       | None     | None | Node.js 8.5.0 before 8.6.0 allows remote attackers to access unintended files, because a change to ".." handling was incompatible with the pathname validation used by unspecified community modules.  |
| Node.js | 20.17.0 | CVE-2017-15010       | None     | None | A ReDoS (regular expression denial of service) flaw was found in the tough-cookie module before 2.3.3 for Node.js. An attacker that is able to make an HTTP request using a specially crafted cookie may cause the application to consume an excessive amount of CPU.  |
| Node.js | 20.17.0 | CVE-2015-7384        | None     | None | Node.js 4.0.0, 4.1.0, and 4.1.1 allows remote attackers to cause a denial of service.  |
| Node.js | 20.17.0 | CVE-2013-7377        | None     | None | The codem-transcode module before 0.5.0 for Node.js, when fprobe is enabled, allows remote attackers to execute arbitrary commands via a POST request to /probe.   |
| Node.js | 20.17.0 | CVE-2014-3741        | None     | None | The printDirect function in lib/printer.js in the node-printer module 0.0.1 and earlier for Node.js allows remote attackers to execute arbitrary commands via unspecified characters in the lpr command.   |
| Node.js | 20.17.0 | CVE-2014-3744        | None     | None | Directory traversal vulnerability in the st module before 0.2.5 for Node.js allows remote attackers to read arbitrary files via a %2e%2e (encoded dot dot) in an unspecified path.   |
| Node.js | 20.17.0 | CVE-2017-14919       | None     | None | Node.js before 4.8.5, 6.x before 6.11.5, and 8.x before 8.8.0 allows remote attackers to cause a denial of service (uncaught exception and crash) by leveraging a change in the zlib module 1.2.9 making 8 an invalid value for the windowBits parameter.  |
| Node.js | 20.17.0 | CVE-2017-100021<br>9 | None     | None | npm/KyleRoss windows-cpu all versions vulnerable to command injection resulting in code execution as Node.js user  |
| Node.js | 20.17.0 | CVE-2017-15896       | CRITICAL | 9.1  | Node.js was affected by OpenSSL vulnerability CVE-2017-3737 in regards to the use of SSL_read() due to TLS handshake failure. The result was that an active network attacker could send application data to Node.js using the TLS or HTTP2 modules in a way that bypassed TLS authentication and encryption. |

|         |         |                |        |      |   |
|---------|---------|----------------|--------|------|---|
| Node.js | 20.17.0 | CVE-2017-15897 | LOW    | 3.1  | Node.js had a bug in versions 8.X and 9.X which caused buffers to not be initialized when the encoding for the fill value did not match the encoding specified. For example, 'Buffer.alloc(0x100, "This is not correctly encoded", "hex");' The buffer implementation was updated such that the buffer will be initialized to all zeros in these cases.   |
| Node.js | 20.17.0 | CVE-2018-7651  | None   | None | index.js in the ssri module before 5.2.2 for Node.js is prone to a regular expression denial of service vulnerability in strict mode functionality via a long base64 hash string.   |
| Node.js | 20.17.0 | CVE-2017-18214 | HIGH   | 7.5  | The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.   |
| Node.js | 20.17.0 | CVE-2018-7158  | HIGH   | 7.5  | The "path" module in the Node.js 4.x release line contains a potential regular expression denial of service (ReDoS) vector. The code in question was replaced in Node.js 6.x and later so this vulnerability only impacts all versions of Node.js 4.x. The regular expression, 'splitPathRe', used within the "path" module for the various path parsing functions, including 'path.dirname()', 'path.extname()' and 'path.parse()' was structured in such a way as to allow an attacker to craft a string, that when passed through one of these functions, could take a significant amount of time to evaluate, potentially leading to a full denial of service.  |
| Node.js | 20.17.0 | CVE-2018-7159  | MEDIUM | 5.3  | The HTTP parser in all current versions of Node.js ignores spaces in the 'Content-Length' header, allowing input such as 'Content-Length: 1 2' to be interpreted as having a value of '12'. The HTTP specification does not allow for spaces in the 'Content-Length' value and the Node.js HTTP parser has been brought into line on this particular difference. The security risk of this flaw to Node.js users is considered to be VERY LOW as it is difficult, and may be impossible, to craft an attack that makes use of this flaw in a way that could not already be achieved by supplying an incorrect value for 'Content-Length'. Vulnerabilities may exist in user-code that make incorrect assumptions about the potential accuracy of this value compared to the actual length of the data supplied. Node.js users crafting lower-level HTTP utilities are advised to re-check the length of any input supplied after parsing is complete. |

|         |         |                |      |      |  |
|---------|---------|----------------|------|------|--|
| Node.js | 20.17.0 | CVE-2018-7160  | HIGH | 8.8  | The Node.js inspector, in 6.x and later is vulnerable to a DNS rebinding attack which could be exploited to perform remote code execution. An attack is possible from malicious websites open in a web browser on the same computer, or another computer with network access to the computer running the Node.js process. A malicious website could use a DNS rebinding attack to trick the web browser to bypass same-origin-policy checks and to allow HTTP connections to localhost or to hosts on the local network. If a Node.js process with the debug port active is running on localhost or on a host on the local network, the malicious website could connect to it as a debugger, and get full code execution access. |
| Node.js | 20.17.0 | CVE-2016-10558 | None | None | aerospike is an Aerospike add-on module for Node.js. aerospike versions below 2.4.2 download binary resources over HTTP, which leaves the module vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.  |
| Node.js | 20.17.0 | CVE-2016-10577 | None | None | ibm_db is an asynchronous/synchronous interface for node.js to IBM DB2 and IBM Informix. ibm_db before 1.0.2 downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.  |
| Node.js | 20.17.0 | CVE-2016-10586 | None | None | macaca-chromedriver is a Node.js wrapper for the selenium chromedriver. macaca-chromedriver before 1.0.29 downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.   |
| Node.js | 20.17.0 | CVE-2016-10590 | None | None | cue-sdk-node is a Corsair Cue SDK wrapper for node.js. cue-sdk-node downloads zipped resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested zip file with an attacker controlled zip file if the attacker is on the network or positioned in between the user and the remote server.   |

|         |         |                |          |      |   |
|---------|---------|----------------|----------|------|---|
| Node.js | 20.17.0 | CVE-2016-10698 | None     | None | mystem-fix is a node.js wrapper for MyStem morphology text analyzer by Yandex.ru mystem-fix downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested resources with an attacker controlled copy if the attacker is on the network or positioned in between the user and the remote server.   |
| Node.js | 20.17.0 | CVE-2018-3745  | CRITICAL | 9.1  | atob 2.0.3 and earlier allocates uninitialized Buffers when number is passed in input on Node.js 4.x and below.   |
| Node.js | 20.17.0 | CVE-2016-10536 | None     | None | engine.io-client is the client for engine.io, the implementation of a transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. The vulnerability is related to the way that node.js handles the `rejectUnauthorized` setting. If the value is something that evaluates to false, certificate verification will be disabled. This is problematic as engine.io-client 1.6.8 and earlier passes in an object for settings that includes the rejectUnauthorized property, whether it has been set or not. If the value has not been explicitly changed, it will be passed in as `null`, resulting in certificate verification being turned off. |
| Node.js | 20.17.0 | CVE-2016-10539 | None     | None | negotiator is an HTTP content negotiator for Node.js and is used by many modules and frameworks including Express and Koa. The header for "Accept-Language", when parsed by negotiator 0.6.0 and earlier is vulnerable to Regular Expression Denial of Service via a specially crafted string.  |
| Node.js | 20.17.0 | CVE-2016-10542 | None     | None | ws is a "simple to use, blazing fast and thoroughly tested websocket client, server and console for node.js, up-to-date against RFC-6455". By sending an overly long websocket payload to a `ws` server, it is possible to crash the node process. This affects ws 1.1.0 and earlier.   |
| Node.js | 20.17.0 | CVE-2016-10557 | None     | None | appium-chromedriver is a Node.js wrapper around Chromedriver. Versions below 2.9.4 download binary resources over HTTP, which leaves the module vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.  |

|         |         |                |      |      |  |
|---------|---------|----------------|------|------|--|
| Node.js | 20.17.0 | CVE-2016-10571 | None | None | bkjs-wand is imagemagick wand support for node.js and backendjs bkjs-wand versions lower than 0.3.2 download binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.      |
| Node.js | 20.17.0 | CVE-2016-10575 | None | None | Kindlegen is a simple Node.js wrapper of the official kindlegen program. Kindlegen versions before 1.1.0 download binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server. |
| Node.js | 20.17.0 | CVE-2016-10582 | None | None | closurecompiler is a Closure Compiler for node.js. closurecompiler downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.                                      |
| Node.js | 20.17.0 | CVE-2016-10594 | None | None | ipip is a Node.js module to query geolocation information for an IP or domain, based on database by ipip.net. ipip downloads data resources over HTTP, which leaves it vulnerable to MITM attacks.   |
| Node.js | 20.17.0 | CVE-2016-10596 | None | None | imageoptim is a Node.js wrapper for some images compression algorithms. imageoptim downloads zipped resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested tarball with an attacker controlled tarball if the attacker is on the network or positioned in between the user and the remote server.                    |
| Node.js | 20.17.0 | CVE-2016-10598 | None | None | arrayfire-js is a module for ArrayFire for the Node.js platform. arrayfire-js downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.                           |

|         |         |                |      |      |  |
|---------|---------|----------------|------|------|--|
| Node.js | 20.17.0 | CVE-2016-10599 | None | None | sauce-connect is a Node.js wrapper over the SauceLabs SauceConnect.jar program for establishing a secure tunnel for intranet testing. sauce-connect downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server. |
| Node.js | 20.17.0 | CVE-2016-10608 | None | None | robot-js is a module for native system automation for node.js. robot-js downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.   |
| Node.js | 20.17.0 | CVE-2016-10613 | None | None | bionode-sra is a Node.js wrapper for SRA Toolkit. bionode-sra downloads data resources over HTTP, which leaves it vulnerable to MITM attacks.  |
| Node.js | 20.17.0 | CVE-2016-10614 | None | None | httpsync is a port of libcurl to node.js. httpsync downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.  |
| Node.js | 20.17.0 | CVE-2016-10623 | None | None | macaca-chromedriver-zxa is a Node.js wrapper for the selenium chromedriver. macaca-chromedriver-zxa downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.   |
| Node.js | 20.17.0 | CVE-2016-10633 | None | None | dwebp-bin is a dwebp node.js wrapper that convert WebP into PNG. dwebp-bin downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.  |

|         |         |                |      |      |  |
|---------|---------|----------------|------|------|--|
| Node.js | 20.17.0 | CVE-2016-10651 | None | None | webdriver-launcher is a Node.js Selenium Webdriver Launcher. webdriver-launcher downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.   |
| Node.js | 20.17.0 | CVE-2016-10664 | None | None | mystem is a Node.js wrapper for MyStem morphology text analyzer by Yandex.ru mystem downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server.   |
| Node.js | 20.17.0 | CVE-2016-10677 | None | None | google-closure-tools-latest is a Node.js module wrapper for downloading the latest version of the Google Closure tools google-closure-tools-latest downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested resources with an attacker controlled copy if the attacker is on the network or positioned in between the user and the remote server. |
| Node.js | 20.17.0 | CVE-2017-16007 | None | None | node-jose is a JavaScript implementation of the JSON Object Signing and Encryption (JOSE) for current web browsers and node.js-based servers. node-jose earlier than version 0.9.3 is vulnerable to an invalid curve attack. This allows an attacker to recover the private secret key when JWE with Key Agreement with Elliptic Curve Diffie-Hellman Ephemeral Static (ECDH-ES) is used.  |
| Node.js | 20.17.0 | CVE-2017-16019 | None | None | GitBook is a command line tool (and Node.js library) for building beautiful books using GitHub/Git and Markdown (or AsciiDoc). Stored Cross-Site-Scripting (XSS) is possible in GitBook before 3.2.2 by including code outside of backticks in any ebook. This code will be executed on the online reader.   |
| Node.js | 20.17.0 | CVE-2017-16184 | None | None | scott-blanch-weather-app is a sample Node.js app using Express 4. scott-blanch-weather-app is vulnerable to a directory traversal issue, giving an attacker access to the filesystem by placing "../" in the url.  |

|         |         |                |      |      |   |
|---------|---------|----------------|------|------|---|
| Node.js | 20.17.0 | CVE-2018-7161  | HIGH | 7.5  | All versions of Node.js 8.x, 9.x, and 10.x are vulnerable and the severity is HIGH. An attacker can cause a denial of service (DoS) by causing a node server providing an http2 server to crash. This can be accomplished by interacting with the http2 server in a manner that triggers a cleanup bug where objects are used in native code after they are no longer available. This has been addressed by updating the http2 implementation.      |
| Node.js | 20.17.0 | CVE-2018-7162  | HIGH | 7.5  | All versions of Node.js 9.x and 10.x are vulnerable and the severity is HIGH. An attacker can cause a denial of service (DoS) by causing a node process which provides an http server supporting TLS server to crash. This can be accomplished by sending duplicate/unexpected messages during the handshake. This vulnerability has been addressed by updating the TLS implementation.   |
| Node.js | 20.17.0 | CVE-2018-7164  | HIGH | 7.5  | Node.js versions 9.7.0 and later and 10.x are vulnerable and the severity is MEDIUM. A bug introduced in 9.7.0 increases the memory consumed when reading from the network into JavaScript using the net.Socket object directly as a stream. An attacker could use this cause a denial of service by sending tiny chunks of data in short succession. This vulnerability was restored by reverting to the prior behaviour.                          |
| Node.js | 20.17.0 | CVE-2018-7167  | HIGH | 7.5  | Calling Buffer.fill() or Buffer.alloc() with some parameters can lead to a hang which could result in a Denial of Service. In order to address this vulnerability, the implementations of Buffer.alloc() and Buffer.fill() were updated so that they zero fill instead of hanging in these cases. All versions of Node.js 6.x (LTS "Boron"), 8.x (LTS "Carbon"), and 9.x are vulnerable. All versions of Node.js 10.x (Current) are NOT vulnerable. |
| Node.js | 20.17.0 | CVE-2018-12519 | None | None | An issue was discovered in ShopNx through 2017-11-17. The vulnerability allows a remote attacker to upload any malicious file to a Node.js application. An attacker can upload a malicious HTML file that contains a JavaScript payload to steal a user's credentials.  |
| Node.js | 20.17.0 | CVE-2018-3754  | None | None | Node.js third-party module query-mysql versions 0.0.0, 0.0.1, and 0.0.2 are vulnerable to an SQL injection vulnerability due to lack of user input sanitization. This may allow an attacker to run arbitrary SQL queries when fetching data from database.  |

|         |         |                |      |      |  |
|---------|---------|----------------|------|------|--|
| Node.js | 20.17.0 | CVE-2018-13797 | None | None | The macaddress module before 0.2.9 for Node.js is prone to an arbitrary command injection flaw, due to allowing unsanitized input to an exec (rather than execFile) call.  |
| Node.js | 20.17.0 | CVE-2018-12115 | None | None | In all versions of Node.js prior to 6.14.4, 8.11.4 and 10.9.0 when used with UCS-2 encoding (recognized by Node.js under the names <code>'ucs2'</code> , <code>'ucs-2'</code> , <code>'utf16le'</code> and <code>'utf-16le'</code> ), <code>Buffer#write()</code> can be abused to write outside of the bounds of a single <code>Buffer</code> . Writes that start from the second-to-last position of a buffer cause a miscalculation of the maximum length of the input bytes to be written.   |
| Node.js | 20.17.0 | CVE-2018-7166  | HIGH | 7.5  | In all versions of Node.js 10 prior to 10.9.0, an argument processing flaw can cause <code>Buffer.alloc()</code> to return uninitialized memory. This method is intended to be safe and only return initialized, or cleared, memory. The third argument specifying <code>'encoding'</code> can be passed as a number, this is misinterpreted by <code>Buffer's</code> internal "fill" method as the <code>'start'</code> to a fill operation. This flaw may be abused where <code>Buffer.alloc()</code> arguments are derived from user input to return uncleared memory blocks that may contain sensitive information.                            |
| Node.js | 20.17.0 | CVE-2018-16460 | None | None | A command Injection in ps package versions <1.0.0 for Node.js allowed arbitrary commands to be executed when attacker controls the PID.  |
| Node.js | 20.17.0 | CVE-2018-12116 | HIGH | 7.5  | Node.js: All versions prior to Node.js 6.15.0 and 8.14.0: HTTP request splitting: If Node.js can be convinced to use unsanitized user-provided Unicode data for the <code>'path'</code> option of an HTTP request, then data can be provided which will trigger a second, unexpected, and user-defined HTTP request to made to the same server.  |
| Node.js | 20.17.0 | CVE-2018-12120 | HIGH | 8.1  | Node.js: All versions prior to Node.js 6.15.0: Debugger port 5858 listens on any interface by default: When the debugger is enabled with <code>'node --debug'</code> or <code>'node debug'</code> , it listens to port 5858 on all interfaces by default. This may allow remote computers to attach to the debug port and evaluate arbitrary JavaScript. The default interface is now localhost. It has always been possible to start the debugger on a specific interface, such as <code>'node --debug=localhost'</code> . The debugger was removed in Node.js 8 and replaced with the inspector, so no versions from 8 and later are vulnerable. |

|         |         |                |        |      |  |
|---------|---------|----------------|--------|------|--|
| Node.js | 20.17.0 | CVE-2018-12121 | HIGH   | 7.5  | Node.js: All versions prior to Node.js 6.15.0, 8.14.0, 10.14.0 and 11.3.0: Denial of Service with large HTTP headers: By using a combination of many requests with maximum sized headers (almost 80 KB per connection), and carefully timed completion of the headers, it is possible to cause the HTTP server to abort from heap allocation failure. Attack potential is mitigated by the use of a load balancer or other proxy layer.  |
| Node.js | 20.17.0 | CVE-2018-12122 | HIGH   | 7.5  | Node.js: All versions prior to Node.js 6.15.0, 8.14.0, 10.14.0 and 11.3.0: Slowloris HTTP Denial of Service: An attacker can cause a Denial of Service (DoS) by sending headers very slowly keeping HTTP or HTTPS connections and associated resources alive for a long period of time.  |
| Node.js | 20.17.0 | CVE-2018-12123 | MEDIUM | 4.3  | Node.js: All versions prior to Node.js 6.15.0, 8.14.0, 10.14.0 and 11.3.0: Hostname spoofing in URL parser for javascript protocol: If a Node.js application is using url.parse() to determine the URL hostname, that hostname can be spoofed by using a mixed case "javascript:" (e.g. "javAScript:") protocol (other protocols are not affected). If security decisions are made about the URL based on the hostname, they may be incorrect.   |
| Node.js | 20.17.0 | CVE-2018-11798 | None   | None | The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webserver's docroot path.   |
| Node.js | 20.17.0 | CVE-2019-10061 | None   | None | utils/find-opencv.js in node-opencv (aka OpenCV bindings for Node.js) prior to 6.1.0 is vulnerable to Command Injection. It does not validate user input allowing attackers to execute arbitrary commands.   |
| Node.js | 20.17.0 | CVE-2019-5737  | HIGH   | 7.5  | In Node.js including 6.x before 6.17.0, 8.x before 8.15.1, 10.x before 10.15.2, and 11.x before 11.10.1, an attacker can cause a Denial of Service (DoS) by establishing an HTTP or HTTPS connection in keep-alive mode and by sending headers very slowly. This keeps the connection and associated resources alive for a long period of time. Potential attacks are mitigated by the use of a load balancer or other proxy layer. This vulnerability is an extension of CVE-2018-12121, addressed in November and impacts all active Node.js release lines including 6.x before 6.17.0, 8.x before 8.15.1, 10.x before 10.15.2, and 11.x before 11.10.1. |

|         |         |                |          |      |   |
|---------|---------|----------------|----------|------|---|
| Node.js | 20.17.0 | CVE-2019-5739  | HIGH     | 7.5  | Keep-alive HTTP and HTTPS connections can remain open and inactive for up to 2 minutes in Node.js 6.16.0 and earlier. Node.js 8.0.0 introduced a dedicated <code>server.keepAliveTimeout</code> which defaults to 5 seconds. The behavior in Node.js 6.16.0 and earlier is a potential Denial of Service (DoS) attack vector. Node.js 6.17.0 introduces <code>server.keepAliveTimeout</code> and the 5-second default.        |
| Node.js | 20.17.0 | CVE-2018-18524 | None     | None | Evernote 6.15 on Windows has an incorrectly repaired stored XSS vulnerability. An attacker can use this XSS issue to inject Node.js code under Present mode. After a victim opens an affected note under Present mode, the attacker can read the victim's files and achieve remote execution command on the victim's computer.  |
| Node.js | 20.17.0 | CVE-2019-10157 | None     | None | It was found that Keycloak's Node.js adapter before version 4.8.3 did not properly verify the web token received from the server in its backchannel logout . An attacker with local access could use this to construct a malicious web token setting an NBF parameter that could prevent user access indefinitely.  |
| Node.js | 20.17.0 | CVE-2019-14939 | None     | None | An issue was discovered in the mysql (aka mysqljs) module 2.17.1 for Node.js. The LOAD DATA LOCAL INFILE option is open by default.   |
| Node.js | 20.17.0 | CVE-2019-13030 | HIGH     | 8.2  | eQ-3 Homematic CCU3 AddOn 'Mediola NEO Server for Homematic CCU3' prior to 2.4.5 allows uncontrolled admin access to start or stop the Node.js process, resulting in the ability to obtain mediola configuration details. This is related to improper access control for addons configuration pages and a missing check in <code>rc.d/97NeoServer</code> .  |
| Node.js | 20.17.0 | CVE-2019-15138 | HIGH     | 7.5  | The <code>html-pdf</code> package 2.2.0 for Node.js has an arbitrary file read vulnerability via an HTML file that uses <code>XMLHttpRequest</code> to access a <code>file:///</code> URL.  |
| Node.js | 20.17.0 | CVE-2019-17592 | HIGH     | 7.5  | The <code>csv-parse</code> module before 4.4.6 for Node.js is vulnerable to Regular Expression Denial of Service. The <code>__isInt()</code> function contains a malformed regular expression that processes large crafted input very slowly. This is triggered when using the <code>cast</code> option.  |
| Node.js | 20.17.0 | CVE-2019-17625 | CRITICAL | 9.0  | There is a stored XSS in Rambox 0.6.9 that can lead to code execution. The XSS is in the name field while adding/editing a service. The problem occurs due to incorrect sanitization of the name field when being processed and stored. This allows a user to craft a payload for Node.js and Electron, such as an <code>exec</code> of OS commands within the <code>onerror</code> attribute of an <code>IMG</code> element. |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2019-17606 | MEDIUM               | 6.1        | The Post editor functionality in the hexo-admin plugin versions 2.3.0 and earlier for Node.js is vulnerable to stored XSS via the content of a post.  |
| Node.js | 20.17.0 | CVE-2019-16769 | ['MEDIUM', 'MEDIUM'] | [4.2, 5.4] | The serialize-javascript npm package before version 2.1.1 is vulnerable to Cross-site Scripting (XSS). It does not properly mitigate against unsafe characters in serialized regular expressions. This vulnerability is not affected on Node.js environment since Node.js's implementation of RegExp.prototype.toString() backslash-escapes all forward slashes in regular expressions. If serialized data of regular expression objects are used in an environment other than Node.js, it is affected by this vulnerability. |
| Node.js | 20.17.0 | CVE-2019-16772 | ['LOW', 'MEDIUM']    | [3.1, 6.1] | The serialize-to-js NPM package before version 3.0.1 is vulnerable to Cross-site Scripting (XSS). It does not properly mitigate against unsafe characters in serialized regular expressions. This vulnerability is not affected on Node.js environment since Node.js's implementation of RegExp.prototype.toString() backslash-escapes all forward slashes in regular expressions. If serialized data of regular expression objects are used in an environment other than Node.js, it is affected by this vulnerability.      |
| Node.js | 20.17.0 | CVE-2019-19729 | HIGH                 | 7.5        | An issue was discovered in the BSON ObjectId (aka bson-objectid) package 1.3.0 for Node.js. ObjectId() allows an attacker to generate a malformed objectid by inserting an additional property to the user-input, because bson-objectid will return early if it detects _bsontype==ObjectId in the user-input object. As a result, objects in arbitrary forms can bypass formatting if they have a valid bsontype.  |
| Node.js | 20.17.0 | CVE-2019-19771 | HIGH                 | 8.8        | The lodahs package 0.0.1 for Node.js is a Trojan horse, and may have been installed by persons who mistyped the lodash package name. In particular, the Trojan horse finds and exfiltrates cryptocurrency wallets.  |
| Node.js | 20.17.0 | CVE-2014-3743  | MEDIUM               | 6.1        | Multiple cross-site scripting (XSS) vulnerabilities in the Marked module before 0.3.1 for Node.js allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) gfm codeblocks (language) or (2) javascript url's.   |

|         |         |                |          |     |   |
|---------|---------|----------------|----------|-----|---|
| Node.js | 20.17.0 | CVE-2020-6836  | CRITICAL | 9.8 | grammar-parser.json in the hot-formula-parser package before 3.0.1 for Node.js is vulnerable to arbitrary code injection. The package fails to sanitize values passed to the parse function and concatenates them in an eval call. If a value of the formula is taken from user-controlled input, it may allow attackers to run arbitrary commands on the server. |
| Node.js | 20.17.0 | CVE-2019-15604 | HIGH     | 7.5 | Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate  |
| Node.js | 20.17.0 | CVE-2019-15605 | CRITICAL | 9.8 | HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed  |
| Node.js | 20.17.0 | CVE-2013-7378  | CRITICAL | 9.8 | scripts/email.coffee in the Hubot Scripts module before 2.4.4 for Node.js allows remote attackers to execute arbitrary commands.  |
| Node.js | 20.17.0 | CVE-2013-7381  | CRITICAL | 9.8 | libnotify before 1.0.4 for Node.js allows remote attackers to execute arbitrary commands via unspecified characters in a call to libnotify.notify.  |
| Node.js | 20.17.0 | CVE-2020-11883 | MEDIUM   | 5.3 | In Divante vue-storefront-api through 1.11.1 and storefront-api through 1.0-rc.1, as used in VueStorefront PWA, unexpected HTTP requests lead to an exception that discloses the error stack trace, with absolute file paths and Node.js module names.  |
| Node.js | 20.17.0 | CVE-2020-12265 | CRITICAL | 9.8 | The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.   |
| Node.js | 20.17.0 | CVE-2020-13110 | HIGH     | 7.8 | The kerberos package before 1.0.0 for Node.js allows arbitrary code execution and privilege escalation via injection of malicious DLLs through use of the kerberos_sspi LoadLibrary() method, because of a DLL path search.   |
| Node.js | 20.17.0 | CVE-2020-13822 | HIGH     | 7.7 | The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading '\0' bytes, or integer overflows. This could conceivably have a security-relevant impact if an application relied on a single canonical signature.   |
| Node.js | 20.17.0 | CVE-2017-18869 | LOW      | 2.5 | A TOCTOU issue in the chownr package before 1.1.0 for Node.js 10.10 could allow a local attacker to trick it into descending into unintended directories via symlink attacks.   |

|         |         |                |                          |             |   |
|---------|---------|----------------|--------------------------|-------------|---|
| Node.js | 20.17.0 | CVE-2020-14966 | HIGH                     | 7.5         | An issue was discovered in the jsrsasign package through 8.0.18 for Node.js. It allows a malleability in ECDSA signatures by not checking overflows in the length of a sequence and '0' characters appended or prepended to an integer. The modified signatures are verified as valid. This could have a security-relevant impact if an application relied on a single canonical signature.   |
| Node.js | 20.17.0 | CVE-2020-14967 | CRITICAL                 | 9.8         | An issue was discovered in the jsrsasign package before 8.0.18 for Node.js. Its RSA PKCS1 v1.5 decryption implementation does not detect ciphertext modification by prepending '\0' bytes to ciphertexts (it decrypts modified ciphertexts without error). An attacker might prepend these bytes with the goal of triggering memory corruption issues.  |
| Node.js | 20.17.0 | CVE-2020-14968 | CRITICAL                 | 9.8         | An issue was discovered in the jsrsasign package before 8.0.17 for Node.js. Its RSASSA-PSS (RSA-PSS) implementation does not detect signature manipulation/modification by prepending '\0' bytes to a signature (it accepts these modified signatures as valid). An attacker can abuse this behavior in an application by creating multiple valid signatures where only one signature should exist. Also, an attacker might prepend these bytes with the goal of triggering memory corruption issues. |
| Node.js | 20.17.0 | CVE-2018-21268 | ['CRITICAL', 'CRITICAL'] | [10.0, 9.8] | The traceroute (aka node-traceroute) package through 1.0.0 for Node.js allows remote command injection via the host parameter. This occurs because the Child.exec() method, which is considered to be not entirely safe, is used. In particular, an OS command can be placed after a newline character.   |
| Node.js | 20.17.0 | CVE-2020-15779 | HIGH                     | 7.5         | A Path Traversal issue was discovered in the socket.io-file package through 2.0.31 for Node.js. The socket.io-file::createFile message uses path.join with ../ in the name option, and the uploadDir and rename options determine the path.   |
| Node.js | 20.17.0 | CVE-2020-24660 | CRITICAL                 | 9.8         | An issue was discovered in LemonLDAP::NG through 2.0.8, when NGINX is used. An attacker may bypass URL-based access control to protected Virtual Hosts by submitting a non-normalized URI. This also affects versions before 0.5.2 of the "Lemonldap::NG handler for Node.js" package.  |

|         |         |                |      |     |   |
|---------|---------|----------------|------|-----|---|
| Node.js | 20.17.0 | CVE-2020-8201  | HIGH | 7.4 | Node.js < 12.18.4 and < 14.11 can be exploited to perform HTTP desync attacks and deliver malicious payloads to unsuspecting users. The payloads can be crafted by an attacker to hijack user sessions, poison cookies, perform clickjacking, and a multitude of other attacks depending on the architecture of the underlying system. The attack was possible due to a bug in processing of carrier-return symbols in the HTTP header names.       |
| Node.js | 20.17.0 | CVE-2020-8251  | HIGH | 7.5 | Node.js < 14.11.0 is vulnerable to HTTP denial of service (DoS) attacks based on delayed requests submission which can make the server unable to accept new connections.  |
| Node.js | 20.17.0 | CVE-2020-8252  | HIGH | 7.8 | The implementation of realpath in libuv < 10.22.1, < 12.18.4, and < 14.9.0 used within Node.js incorrectly determined the buffer size which can result in a buffer overflow if the resolved path is longer than 256 bytes.  |
| Node.js | 20.17.0 | CVE-2020-24807 | HIGH | 7.8 | The socket.io-file package through 2.0.31 for Node.js relies on client-side validation of file types, which allows remote attackers to execute arbitrary code by uploading an executable file via a modified JSON name field. NOTE: This vulnerability only affects products that are no longer supported by the maintainer   |
| Node.js | 20.17.0 | CVE-2020-13536 | HIGH | 7.8 | An exploitable local privilege elevation vulnerability exists in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary. By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.Js scripts to start additional application functionality.  |
| Node.js | 20.17.0 | CVE-2020-13537 | HIGH | 7.8 | An exploitable local privilege elevation vulnerability exists in the file system permissions of Moxa MXView series 3.1.8 installation. Depending on the vector chosen, an attacker can either add code to a script or replace a binary. By default MXViewService, which starts as a NT SYSTEM authority user executes a series of Node.Js scripts to start additional application functionality and among them the mosquito executable is also run. |
| Node.js | 20.17.0 | CVE-2020-8277  | HIGH | 7.5 | A Node.js application that allows an attacker to trigger a DNS request for a host of their choice could trigger a Denial of Service in versions < 15.2.1, < 14.15.1, and < 12.19.1 by getting the application to resolve a DNS record with a larger number of responses. This is fixed in 15.2.1, 14.15.1, and 12.19.1.   |

|         |         |                |                    |            |   |
|---------|---------|----------------|--------------------|------------|---|
| Node.js | 20.17.0 | CVE-2018-21270 | MEDIUM             | 6.5        | Versions less than 0.0.6 of the Node.js stringstream module are vulnerable to an out-of-bounds read because of allocation of uninitialized buffers when a number is passed in the input stream (when using Node.js 4.x).  |
| Node.js | 20.17.0 | CVE-2020-26288 | ['HIGH', 'MEDIUM'] | [7.7, 6.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. It is an npm package "parse-server". In Parse Server before version 4.5.0, user passwords involved in LDAP authentication are stored in cleartext. This is fixed in version 4.5.0 by stripping password after authentication to prevent cleartext password storage.   |
| Node.js | 20.17.0 | CVE-2020-8265  | HIGH               | 8.1        | Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 are vulnerable to a use-after-free bug in its TLS implementation. When writing to a TLS enabled socket, node::StreamBase::Write calls node::TLSSWrap::DoWrite with a freshly allocated WriteWrap object as first argument. If the DoWrite method does not return an error, this object is passed back to the caller as part of a StreamWriteResult structure. This may be exploited to corrupt memory leading to a Denial of Service or potentially other exploits. |
| Node.js | 20.17.0 | CVE-2020-8287  | MEDIUM             | 6.5        | Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request (for example, two Transfer-Encoding header fields). In this case, Node.js identifies the first header field and ignores the second. This can lead to HTTP Request Smuggling.  |
| Node.js | 20.17.0 | CVE-2021-3190  | CRITICAL           | 9.8        | The async-git package before 1.13.2 for Node.js allows OS Command Injection via shell metacharacters, as demonstrated by git.reset and git.tag.   |
| Node.js | 20.17.0 | CVE-2021-26276 | MEDIUM             | 5.3        | scripts/cli.js in the GoDaddy node-config-shield (aka Config Shield) package before 0.2.2 for Node.js calls eval when processing a set command. NOTE: the vendor reportedly states that this is not a vulnerability. The set command was not intended for use with untrusted data   |
| Node.js | 20.17.0 | CVE-2021-27185 | CRITICAL           | 9.8        | The samba-client package before 4.0.0 for Node.js allows command injection because of the use of process.exec.  |
| Node.js | 20.17.0 | CVE-2021-27191 | HIGH               | 7.5        | The get-ip-range package before 4.0.0 for Node.js is vulnerable to denial of service (DoS) if the range is untrusted input. An attacker could send a large range (such as 128.0.0.0/1) that causes resource exhaustion.   |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-21315 | ['HIGH', 'HIGH']     | [7.1, 7.8] | The System Information Library for Node.JS (npm package "systeminformation") is an open source collection of functions to retrieve detailed hardware, system and OS information. In systeminformation before version 5.3.1 there is a command injection vulnerability. Problem was fixed in version 5.3.1. As a workaround instead of upgrading, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() ... do only allow strings, reject any arrays. String sanitation works as expected.  |
| Node.js | 20.17.0 | CVE-2021-27405 | HIGH                 | 7.5        | A ReDoS (regular expression denial of service) flaw was found in the @progfay/scrapbox-parser package before 6.0.3 for Node.js.   |
| Node.js | 20.17.0 | CVE-2021-3189  | MEDIUM               | 6.1        | The slashify package 1.0.0 for Node.js allows open-redirect attacks, as demonstrated by a localhost:3000///example.com/ substring.  |
| Node.js | 20.17.0 | CVE-2020-27543 | HIGH                 | 7.5        | The restify-paginate package 0.0.5 for Node.js allows remote attackers to cause a Denial-of-Service by omitting the HTTP Host header. A Restify-based web service would crash with an uncaught exception.   |
| Node.js | 20.17.0 | CVE-2021-20327 | ['MEDIUM', 'MEDIUM'] | [6.4, 6.8] | A specific version of the Node.js mongodb-client-encryption module does not perform correct validation of the KMS server's certificate. This vulnerability in combination with a privileged network position active MITM attack could result in interception of traffic between the Node.js driver and the KMS service rendering client-side field level encryption (CSFLE) ineffective. This issue was discovered during internal testing and affects mongodb-client-encryption module version 1.2.0, which was available from 2021-Jan-29 and deprecated in the NPM Registry on 2021-Feb-04. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services from applications residing inside the AWS, GCP, and Azure network fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don't use Field Level Encryption. This issue affects MongoDB Node.js Driver mongodb-client-encryption module version 1.2.0 |
| Node.js | 20.17.0 | CVE-2021-27884 | MEDIUM               | 5.1        | Weak JSON Web Token (JWT) signing secret generation in YMFE YApi through 1.9.2 allows recreation of other users' JWT tokens. This occurs because Math.random in Node.js is used.  |

|         |         |                |                           |               |   |
|---------|---------|----------------|---------------------------|---------------|---|
| Node.js | 20.17.0 | CVE-2021-21353 | ['MEDIUM',<br>'CRITICAL'] | [6.8,<br>9.0] | Pug is an npm package which is a high-performance template engine. In pug before version 3.0.1, if a remote attacker was able to control the `pretty` option of the pug compiler, e.g. if you spread a user provided object such as the query parameters of a request into the pug template inputs, it was possible for them to achieve remote code execution on the node.js backend. This is fixed in version 3.0.1. This advisory applies to multiple pug packages including "pug", "pug-code-gen". pug-code-gen has a backported fix at version 2.0.3. This advisory is not exploitable if there is no way for un-trusted input to be passed to pug as the `pretty` option, e.g. if you compile templates in advance before applying user input to them, you do not need to upgrade. |
| Node.js | 20.17.0 | CVE-2021-22883 | HIGH                      | 7.5           | Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to a denial of service attack when too many connection attempts with an 'unknownProtocol' are established. This leads to a leak of file descriptors. If a file descriptor limit is configured on the system, then the server is unable to accept new connections and prevent the process also from opening, e.g. a file. If no file descriptor limit is configured, then this lead to an excessive memory usage and cause the system to run out of memory.  |
| Node.js | 20.17.0 | CVE-2021-22884 | HIGH                      | 7.5           | Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to DNS rebinding attacks as the whitelist includes <code>localhost6</code> . When <code>localhost6</code> is not present in <code>/etc/hosts</code> , it is just an ordinary domain that is resolved via DNS, i.e., over network. If the attacker controls the victim's DNS server or can spoof its responses, the DNS rebinding protection can be bypassed by using the <code>localhost6</code> domain. As long as the attacker uses the <code>localhost6</code> domain, they can still apply the attack described in CVE-2018-7160.   |

|         |         |                |                    |            |  |
|---------|---------|----------------|--------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-21368 | ['MEDIUM', 'HIGH'] | [6.7, 8.8] | <p>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__.</p> <p>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 "pro...</p> |
| Node.js | 20.17.0 | CVE-2021-28092 | HIGH               | 7.5        | <p>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.</p>   |
| Node.js | 20.17.0 | CVE-2021-21383 | ['HIGH', 'MEDIUM'] | [7.6, 5.4] | <p>Wiki.js an open-source wiki app built on Node.js. Wiki.js before version 2.5.191 is vulnerable to stored cross-site scripting through mustache expressions in code blocks. This vulnerability exists due to mustache expressions being parsed by Vue during content injection even though it is contained within a `<pre>` element. By creating a crafted wiki page, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the page is viewed by other users. For an example see referenced GitHub Security Advisory. Commit 5ffa189383dd716f12b56b8cae2ba0d075996cf1 fixes this vulnerability by adding the v-pre directive to all `<pre>` tags during the render.</pre></pre></p>  |
| Node.js | 20.17.0 | CVE-2021-26275 | CRITICAL           | 9.8        | <p>The eslint-fixer package through 0.1.5 for Node.js allows command injection via shell metacharacters to the fix function. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The ozum/eslint-fixer GitHub repository has been intentionally deleted</p>   |

|         |         |                |                    |            |   |
|---------|---------|----------------|--------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-29418 | MEDIUM             | 5.3        | The netmask package before 2.0.1 for Node.js mishandles certain unexpected characters in an IP address string, such as an octal digit of 9. This (in some situations) allows attackers to bypass access control that is based on IP addresses. NOTE: this issue exists because of an incomplete fix for CVE-2021-28918.   |
| Node.js | 20.17.0 | CVE-2021-30246 | CRITICAL           | 9.1        | In the jsrsasign package through 10.1.13 for Node.js, some invalid RSA PKCS#1 v1.5 signatures are mistakenly recognized to be valid. NOTE: there is no known practical attack.  |
| Node.js | 20.17.0 | CVE-2021-26073 | ['HIGH', 'HIGH']   | [7.7, 7.7] | Broken Authentication in Atlassian Connect Express (ACE) from version 3.0.2 before version 6.6.0: Atlassian Connect Express is a Node.js package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Express app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Express versions from 3.0.2 before 6.6.0 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app. |
| Node.js | 20.17.0 | CVE-2021-31597 | CRITICAL           | 9.4        | The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected.   |
| Node.js | 20.17.0 | CVE-2021-29469 | ['MEDIUM', 'HIGH'] | [5.3, 7.5] | Node-redis is a Node.js Redis client. Before version 3.1.1, when a client is in monitoring mode, the regex begin used to detected monitor messages could cause exponential backtracking on some strings. This issue could lead to a denial of service. The issue is patched in version 3.1.1.   |
| Node.js | 20.17.0 | CVE-2021-21414 | ['HIGH', 'HIGH']   | [7.7, 7.2] | Prisma is an open source ORM for Node.js & TypeScript. As of today, we are not aware of any Prisma users or external consumers of the `@prisma/sdk` package who are affected by this security vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. It only affects the `getPackedPackage` function and this function is not advertised and only used for tests & building our CLI, no malicious code was found after checking our codebase.   |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-21388 | ['HIGH', 'CRITICAL'] | [8.9, 9.8] | systeminformation is an open source system and OS information library for node.js. A command injection vulnerability has been discovered in versions of systeminformation prior to 5.6.4. The issue has been fixed with a parameter check on user input. Please upgrade to version >= 5.6.4. If you cannot upgrade, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() and other commands. Only allow strings, reject any arrays. String sanitation works as expected.   |
| Node.js | 20.17.0 | CVE-2021-29484 | ['MEDIUM', 'MEDIUM'] | [6.8, 6.1] | Ghost is a Node.js CMS. An unused endpoint added during the development of 4.0.0 has left sites vulnerable to untrusted users gaining access to Ghost Admin. Attackers can gain access by getting logged in users to click a link containing malicious code. Users do not need to enter credentials and may not know they've visited a malicious site. Ghost(Pro) has already been patched. We can find no evidence that the issue was exploited on Ghost(Pro) prior to the patch being added. Self-hosters are impacted if running Ghost a version between 4.0.0 and 4.3.2. Immediate action should be taken to secure your site. The issue has been fixed in 4.3.3, all 4.x sites should upgrade as soon as possible. As the endpoint is unused, the patch simply removes it. As a workaround blocking access to /ghost/preview can also mitigate the issue. |
| Node.js | 20.17.0 | CVE-2021-28860 | CRITICAL             | 9.1        | In Node.js mixme, prior to v0.5.1, an attacker can add or alter properties of an object via '__proto__' through the mutate() and merge() functions. The polluted attribute will be directly assigned to every object in the program. This will put the availability of the program at risk causing a potential denial of service (DoS).  |
| Node.js | 20.17.0 | CVE-2021-29369 | CRITICAL             | 9.8        | The gnuplot package prior to version 0.1.0 for Node.js allows code execution via shell metacharacters in Gnuplot commands.   |
| Node.js | 20.17.0 | CVE-2021-32573 | MEDIUM               | 4.8        | The express-cart package through 1.1.10 for Node.js allows Reflected XSS (for an admin) via a user input field for product options. NOTE: the vendor states that this "would rely on an admin hacking his/her own website.   |
| Node.js | 20.17.0 | CVE-2021-33502 | HIGH                 | 7.5        | The normalize-url package before 4.5.1, 5.x before 5.3.1, and 6.x before 6.0.1 for Node.js has a ReDoS (regular expression denial of service) issue because it has exponential performance for data: URLs.   |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-32624 | ['HIGH', 'MEDIUM']   | [7.5, 5.3] | Keystone 5 is an open source CMS platform to build Node.js applications. This security advisory relates to a newly discovered capability in our query infrastructure to directly or indirectly expose the values of private fields, bypassing the configured access control. This is an access control related oracle attack in that the attack method guides an attacker during their attempt to reveal information they do not have access to. The complexity of completing the attack is limited by some length-dependent behaviors and the fidelity of the exposed information. Under some circumstances, field values or field value meta data can be determined, despite the field or list having `read` access control configured. If you use private fields or lists, you may be impacted. No patches exist at this time. There are no workarounds at this time   |
| Node.js | 20.17.0 | CVE-2021-32640 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | ws is an open source WebSocket client and server library for Node.js. A specially crafted value of the `Sec-WebSocket-Protocol` header can be used to significantly slow down a ws server. The vulnerability has been fixed in ws@7.4.6 ( <a href="https://github.com/websockets/ws/commit/00c425ec77993773d823f018f64a5c44e17023ff">https://github.com/websockets/ws/commit/00c425ec77993773d823f018f64a5c44e17023ff</a> ). In vulnerable versions of ws, the issue can be mitigated by reducing the maximum allowed length of the request headers using the `--max-http-header-size=size` ( <a href="https://nodejs.org/api/cli.html#cli_max_http_header_size_size">https://nodejs.org/api/cli.html#cli_max_http_header_size_size</a> ) and/or the `maxHeaderSize` ( <a href="https://nodejs.org/api/http.html#http_http_createserver_options_requestlistener">https://nodejs.org/api/http.html#http_http_createserver_options_requestlistener</a> ) options. |
| Node.js | 20.17.0 | CVE-2021-33623 | HIGH                 | 7.5        | The trim-newlines package before 3.0.1 and 4.x before 4.0.1 for Node.js has an issue related to regular expression denial-of-service (ReDoS) for the .end() method.   |
| Node.js | 20.17.0 | CVE-2021-33587 | HIGH                 | 7.5        | The css-what package 4.0.0 through 5.0.0 for Node.js does not ensure that attribute parsing has Linear Time Complexity relative to the size of the input.   |
| Node.js | 20.17.0 | CVE-2021-26707 | CRITICAL             | 9.8        | The merge-deep library before 3.0.3 for Node.js can be tricked into overwriting properties of Object.prototype or adding new properties to it. These properties are then inherited by every object in the program, thus facilitating prototype-pollution attacks against applications using this library.   |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-33205 | HIGH                     | 8.8        | Western Digital EdgeRover before 0.25 has an escalation of privileges vulnerability where a low privileged user could load malicious content into directories with higher privileges, because of how Node.js is used. An attacker can gain admin privileges and carry out malicious activities such as creating a fake library and stealing user credentials.  |
| Node.js | 20.17.0 | CVE-2021-32685 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | tEnvoy contains the PGP, NaCl, and PBKDF2 in node.js and the browser (hashing, random, encryption, decryption, signatures, conversions), used by TogaTech.org. In versions prior to 7.0.3, the `verifyWithMessage` method of `tEnvoyNaClSigningKey` always returns `true` for any signature that has a SHA-512 hash matching the SHA-512 hash of the message even if the signature was invalid. This issue is patched in version 7.0.3. As a workaround: In `tenvoy.js` under the `verifyWithMessage` method definition within the `tEnvoyNaClSigningKey` class, ensure that the return statement call to `this.verify` ends in `.verified`.   |
| Node.js | 20.17.0 | CVE-2021-21422 | ['HIGH', 'MEDIUM']       | [8.1, 6.1] | mongo-express is a web-based MongoDB admin interface, written with Node.js and express. 1: As mentioned in this issue: <a href="https://github.com/mongo-express/mongo-express/issues/577">https://github.com/mongo-express/mongo-express/issues/577</a> , when the content of a cell grows larger than supported size, clicking on a row will show full document unescaped, however this needs admin interaction on cell. 2: Data cells identified as media will be rendered as media, without being sanitized. Example of different renders: image, audio, video, etc. As an example of type 1 attack, an unauthorized user who only can send a large amount of data in a field of a document may use a payload with embedded javascript. This could send an export of a collection to the attacker without even an admin knowing. Other types of attacks such as dropping a database/collection are possible. |
| Node.js | 20.17.0 | CVE-2021-22918 | MEDIUM                   | 5.3        | Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when <code>uv__idna_toascii()</code> is used to convert strings to ASCII. The pointer <code>p</code> is read and increased without checking whether it is beyond <code>pe</code> , with the latter holding a pointer to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via <code>uv_getaddrinfo()</code> .  |

|         |         |                |                  |            |  |
|---------|---------|----------------|------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-22921 | HIGH             | 7.8        | Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking.                                |
| Node.js | 20.17.0 | CVE-2021-36716 | HIGH             | 7.5        | A ReDoS (regular expression denial of service) flaw was found in the Segment is-email package before 1.0.1 for Node.js. An attacker that is able to provide crafted input to the isEmail(input) function may cause an application to consume an excessive amount of CPU.   |
| Node.js | 20.17.0 | CVE-2021-22931 | CRITICAL         | 9.8        | Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS, Application crashes due to missing input validation of host names returned by Domain Name Servers in Node.js dns library which can lead to output of wrong hostnames (leading to Domain Hijacking) and injection vulnerabilities in applications using the library. |
| Node.js | 20.17.0 | CVE-2021-22939 | MEDIUM           | 5.3        | If the Node.js https API was used incorrectly and "undefined" was in passed for the "rejectUnauthorized" parameter, no error was returned and connections to servers with an expired certificate would have been accepted.   |
| Node.js | 20.17.0 | CVE-2021-22940 | HIGH             | 7.5        | Node.js before 16.6.1, 14.17.5, and 12.22.5 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.   |
| Node.js | 20.17.0 | CVE-2021-39131 | ['HIGH', 'HIGH'] | [7.5, 7.5] | ced detects character encoding using Google's compact_enc_det library. In ced v0.1.0, passing data types other than `Buffer` causes the Node.js process to crash. The problem has been patched in ced v1.0.0. As a workaround, before passing an argument to ced, verify it's a `Buffer` using `Buffer.isBuffer(obj)`.                                       |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-39138 | ['MEDIUM', 'MEDIUM'] | [4.8, 6.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Developers can use the REST API to signup users and also allow users to login anonymously. Prior to version 4.5.1, when an anonymous user is first signed up using REST, the server creates session incorrectly. Particularly, the `authProvider` field in `_Session` class under `createdWith` shows the user logged in creating a password. If a developer later depends on the `createdWith` field to provide a different level of access between a password user and anonymous user, the server incorrectly classified the session type as being created with a `password`. The server does not currently use `createdWith` to make decisions about internal functions, so if a developer is not using `createdWith` directly, they are not affected. The vulnerability only affects users who depend on `createdWith` by using it directly. The issue is patched in Parse Server version 4.5.1. As a workaround, do not ... |
| Node.js | 20.17.0 | CVE-2021-39157 | ['HIGH', 'HIGH']     | [7.5, 7.5] | detect-character-encoding is an open source character encoding inspection library. In detect-character-encoding v0.6.0 and earlier, data matching no charset causes the Node.js process to crash. The problem has been patched in [detect-character-encoding v0.7.0](https://github.com/sonicdoe/detect-character-encoding/releases/tag/v0.7.0). No workaround are available and all users should update to resolve this issue.  |
| Node.js | 20.17.0 | CVE-2021-39171 | ['MEDIUM', 'HIGH']   | [5.3, 7.5] | Passport-SAML is a SAML 2.0 authentication provider for Passport, the Node.js authentication library. Prior to version 3.1.0, a malicious SAML payload can require transforms that consume significant system resources to process, thereby resulting in reduced or denied service. This would be an effective way to perform a denial-of-service attack. This has been resolved in version 3.1.0. The resolution is to limit the number of allowable transforms to 2.   |
| Node.js | 20.17.0 | CVE-2021-32831 | ['HIGH', 'HIGH']     | [7.5, 7.2] | Total.js framework (npm package total.js) is a framework for Node.js platform written in pure JavaScript similar to PHP's Laravel or Python's Django or ASP.NET MVC. In total.js framework before version 3.4.9, calling the utils.set function with user-controlled values leads to code-injection. This can cause a variety of impacts that include arbitrary code execution. This is fixed in version 3.4.9.  |

|         |         |                |                        |             |   |
|---------|---------|----------------|------------------------|-------------|---|
| Node.js | 20.17.0 | CVE-2021-39187 | ['HIGH', 'HIGH']       | [7.5, 7.5]  | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to version 4.10.3, Parse Server crashes when if a query request contains an invalid value for the `explain` option. This is due to a bug in the MongoDB Node.js driver which throws an exception that Parse Server cannot catch. There is a patch for this issue in version 4.10.3. No workarounds aside from upgrading are known to exist.   |
| Node.js | 20.17.0 | CVE-2021-39192 | ['MEDIUM', 'HIGH']     | [6.5, 7.2]  | Ghost is a Node.js content management system. An error in the implementation of the limits service between versions 4.0.0 and 4.9.4 allows all authenticated users (including contributors) to view admin-level API keys via the integrations API endpoint, leading to a privilege escalation vulnerability. This issue is patched in Ghost version 4.10.0. As a workaround, disable all non-Administrator accounts to prevent API access. It is highly recommended to regenerate all API keys after patching or applying the workaround. |
| Node.js | 20.17.0 | CVE-2020-26300 | ['MEDIUM', 'CRITICAL'] | [5.9, 9.8]  | systeminformation is an npm package that provides system and OS information library for node.js. In systeminformation before version 4.26.2 there is a command injection vulnerability. Problem was fixed in version 4.26.2 with a shell string sanitation fix.   |
| Node.js | 20.17.0 | CVE-2020-26301 | ['HIGH', 'CRITICAL']   | [7.5, 10.0] | ssh2 is client and server modules written in pure JavaScript for node.js. In ssh2 before version 1.4.0 there is a command injection vulnerability. The issue only exists on Windows. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This is fixed in version 1.4.0.  |
| Node.js | 20.17.0 | CVE-2021-41580 | MEDIUM                 | 5.3         | The passport-oauth2 package before 1.6.1 for Node.js mishandles the error condition of failure to obtain an access token. This is exploitable in certain use cases where an OAuth identity provider uses an HTTP 200 status code for authentication-failure error reports, and an application grants authorization upon simply receiving the access token (i.e., does not try to use the token). NOTE: the passport-oauth2 vendor does not consider this a passport-oauth2 vulnerability  |

|         |         |                |          |     |  |
|---------|---------|----------------|----------|-----|--|
| Node.js | 20.17.0 | CVE-2021-41109 | HIGH     | 7.5 | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to version 4.10.4, for regular (non-LiveQuery) queries, the session token is removed from the response, but for LiveQuery payloads it is currently not. If a user has a LiveQuery subscription on the `Parse.User` class, all session tokens created during user sign-ups will be broadcast as part of the LiveQuery payload. A patch in version 4.10.4 removes session tokens from the LiveQuery payload. As a workaround, set `user.acl(new Parse.ACL())` in a beforeSave trigger to make the user private already on sign-up. |
| Node.js | 20.17.0 | CVE-2021-22930 | CRITICAL | 9.8 | Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.   |
| Node.js | 20.17.0 | CVE-2021-42740 | CRITICAL | 9.8 | The shell-quote package before 1.7.3 for Node.js allows command injection. An attacker can inject unescaped shell metacharacters through a regex designed to support Windows drive letters. If the output of this package is passed to a real shell as a quoted argument to a command with exec(), an attacker can inject arbitrary commands. This is because the Windows drive letter regex character class is {A-z} instead of the correct {A-Za-z}. Several shell metacharacters exist in the space between capital letter Z and lower case letter a, such as the backtick character.   |
| Node.js | 20.17.0 | CVE-2021-43571 | CRITICAL | 9.8 | The verify function in the Stark Bank Node.js ECDSA library (ecdsa-node) 1.1.2 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.  |

|         |         |                |                    |            |   |
|---------|---------|----------------|--------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-40828 | ['MEDIUM', 'HIGH'] | [6.3, 8.8] | Connections initialized by the AWS IoT Device SDK v2 for Java (versions prior to 1.3.3), Python (versions prior to 1.5.18), C++ (versions prior to 1.12.7) and Node.js (versions prior to 1.5.1) did not verify server certificate hostname during TLS handshake when overriding Certificate Authorities (CA) in their trust stores on Windows. This issue has been addressed in aws-c-io submodule versions 0.9.13 onward. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.3.3 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.5.18 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on Microsoft Windows. |
| Node.js | 20.17.0 | CVE-2021-40829 | ['MEDIUM', 'HIGH'] | [6.3, 8.8] | Connections initialized by the AWS IoT Device SDK v2 for Java (versions prior to 1.4.2), Python (versions prior to 1.6.1), C++ (versions prior to 1.12.7) and Node.js (versions prior to 1.5.3) did not verify server certificate hostname during TLS handshake when overriding Certificate Authorities (CA) in their trust stores on MacOS. This issue has been addressed in aws-c-io submodule versions 0.10.5 onward. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.4.2 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.6.1 on macOS. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on macOS. Amazon Web Services AWS-C-IO 0.10.4 on macOS.       |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-40830 | ['MEDIUM', 'HIGH']   | [6.3, 8.8] | The AWS IoT Device SDK v2 for Java, Python, C++ and Node.js appends a user supplied Certificate Authority (CA) to the root CAs instead of overriding it on Unix systems. TLS handshakes will thus succeed if the peer can be verified either from the user-supplied CA or the system's default trust-store. Attackers with access to a host's trust stores or are able to compromise a certificate authority already in the host's trust store (note: the attacker must also be able to spoof DNS in this case) may be able to use this issue to bypass CA pinning. An attacker could then spoof the MQTT broker, and either drop traffic and/or respond with the attacker's data, but they would not be able to forward this data on to the MQTT broker because the attacker would still need the user's private keys to authenticate against the MQTT broker. The 'aws_tls_ctx_options_override_default_trust_store_*' function within the aws-c-io submodule has been updated to override the default trust store. This correc... |
| Node.js | 20.17.0 | CVE-2021-40831 | ['MEDIUM', 'HIGH']   | [6.3, 7.2] | The AWS IoT Device SDK v2 for Java, Python, C++ and Node.js appends a user supplied Certificate Authority (CA) to the root CAs instead of overriding it on macOS systems. Additionally, SNI validation is also not enabled when the CA has been overridden. TLS handshakes will thus succeed if the peer can be verified either from the user-supplied CA or the system's default trust-store. Attackers with access to a host's trust stores or are able to compromise a certificate authority already in the host's trust store (note: the attacker must also be able to spoof DNS in this case) may be able to use this issue to bypass CA pinning. An attacker could then spoof the MQTT broker, and either drop traffic and/or respond with the attacker's data, but they would not be able to forward this data on to the MQTT broker because the attacker would still need the user's private keys to authenticate against the MQTT broker. The 'aws_tls_ctx_options_override_default_trust_store_*' function within...       |
| Node.js | 20.17.0 | CVE-2021-43786 | ['CRITICAL', 'HIGH'] | [9.8, 7.5] | Nodebb is an open source Node.js based forum software. In affected versions incorrect logic present in the token verification step unintentionally allowed master token access to the API. The vulnerability has been patch as of v1.18.5. Users are advised to upgrade as soon as possible.   |

|         |         |                |                        |            |   |
|---------|---------|----------------|------------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-43787 | ['CRITICAL', 'MEDIUM'] | [9.0, 6.1] | Nodebb is an open source Node.js based forum software. In affected versions a prototype pollution vulnerability in the uploader module allowed a malicious user to inject arbitrary data (i.e. javascript) into the DOM, theoretically allowing for an account takeover when used in conjunction with a path traversal vulnerability disclosed at the same time as this report. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible.   |
| Node.js | 20.17.0 | CVE-2021-43788 | ['MEDIUM', 'MEDIUM']   | [5.0, 5.0] | Nodebb is an open source Node.js based forum software. Prior to v1.18.5, a path traversal vulnerability was present that allowed users to access JSON files outside of the expected `languages/` directory. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible.   |
| Node.js | 20.17.0 | CVE-2021-43800 | ['HIGH', 'HIGH']       | [7.5, 7.5] | Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git). |
| Node.js | 20.17.0 | CVE-2021-43803 | HIGH                   | 7.5        | Next.js is a React framework. In versions of Next.js prior to 12.0.5 or 11.1.3, invalid or malformed URLs could lead to a server crash. In order to be affected by this issue, the deployment must use Next.js versions above 11.1.0 and below 12.0.5, Node.js above 15.0.0, and next start or a custom server. Deployments on Vercel are not affected, along with similar environments where invalid requests are filtered before reaching Next.js. Versions 12.0.5 and 11.1.3 contain patches for this issue.   |

|         |         |                |                    |            |   |
|---------|---------|----------------|--------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-43842 | MEDIUM             | 5.4        | Wiki.js is a wiki app built on Node.js. Wiki.js versions 2.5.257 and earlier are vulnerable to stored cross-site scripting through a SVG file upload. By creating a crafted SVG file, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the SVG is viewed directly by other users. Scripts do not execute when loaded inside a page via normal `` tags. Commit 5d3e81496fba1f0fbd64eeb855f30f69a9040718 fixes this vulnerability by adding an optional (enabled by default) SVG sanitization step to all file uploads that match the SVG mime type. As a workaround, disable file upload for all non-trusted users. Wiki.js version 2.5.260 is the first production version to contain a patch. Version 2.5.258 is the first development build to contain a patch and is available only as a Docker image as requarks/wiki:canary-2.5.258. |
| Node.js | 20.17.0 | CVE-2021-45459 | CRITICAL           | 9.8        | lib/cmd.js in the node-windows package before 1.0.0-beta.6 for Node.js allows command injection via the PID parameter.  |
| Node.js | 20.17.0 | CVE-2021-43855 | ['HIGH', 'MEDIUM'] | [8.2, 5.4] | Wiki.js is a wiki app built on node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through a SVG file upload made via a custom request with a fake MIME type. By creating a crafted SVG file, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the SVG is viewed directly by other users. Scripts do not execute when loaded inside a page via normal `` tags. The malicious SVG can only be uploaded by crafting a custom request to the server with a fake MIME type. A patch in version 2.5.264 fixes this vulnerability by adding an additional file extension verification check to the optional (enabled by default) SVG sanitization step to all file uploads that match the SVG mime type. As a workaround, disable file upload for all non-trusted users.  |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2021-43856 | ['HIGH', 'MEDIUM']   | [8.2, 5.4] | Wiki.js is a wiki app built on Node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through non-image file uploads for file types that can be viewed directly inline in the browser. By creating a malicious file which can execute inline JS when viewed in the browser (e.g. XML files), a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the file is viewed directly by other users. The file must be opened directly by the user and will not trigger directly in a normal Wiki.js page. A patch in version 2.5.264 fixes this vulnerability by adding an optional (enabled by default) force download flag to all non-image file types, preventing the file from being viewed inline in the browser. As a workaround, disable file upload for all non-trusted users. --- Thanks to @Haxatron for reporting this vulnerability. Initially reported via <a href="https://huntr.dev/bounties/266bff09-00d9-43ca-a4bb-bb54...">https://huntr.dev/bounties/266bff09-00d9-43ca-a4bb-bb54...</a> |
| Node.js | 20.17.0 | CVE-2022-21676 | ['HIGH', 'HIGH']     | [7.5, 7.5] | Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the `engine.io` package starting from version `4.0.0`, including those who uses depending packages like `socket.io`. Versions prior to `4.0.0` are not impacted. A fix has been released for each major branch, namely `4.1.2` for the `4.x.x` branch, `5.2.1` for the `5.x.x` branch, and `6.1.1` for the `6.x.x` branch. There is no known workaround except upgrading to a safe version.   |
| Node.js | 20.17.0 | CVE-2022-21704 | ['MEDIUM', 'MEDIUM'] | [5.5, 5.5] | log4js-node is a port of log4js to node.js. In affected versions default file permissions for log files created by the file, fileSync and dateFile appenders are world-readable (in unix). This could cause problems if log files contain sensitive information. This would affect any users that have not supplied their own permissions for the files via the mode parameter in the config. Users are advised to update.  |

|         |         |                |                    |            |   |
|---------|---------|----------------|--------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-23654 | ['HIGH', 'MEDIUM'] | [8.1, 6.5] | <p>Wiki.js is a wiki app built on Node.js. In affected versions an authenticated user with write access on a restricted set of paths can update a page outside the allowed paths by specifying a different target page ID while keeping the path intact. The access control incorrectly check the path access against the user-provided values instead of the actual path associated to the page ID. Commit <a href="https://github.com/Requarks/wiki/commit/411802ec2f654bb5ed1126c307575b81e2361c6b">https://github.com/Requarks/wiki/commit/411802ec2f654bb5ed1126c307575b81e2361c6b</a> fixes this vulnerability by checking access control on the path associated with the page ID instead of the user-provided value. When the path is different than the current value, a second access control check is then performed on the user-provided path before the move operation.</p> |
| Node.js | 20.17.0 | CVE-2021-44531 | HIGH               | 7.4        | <p>Accepting arbitrary Subject Alternative Name (SAN) types, unless a PKI is specifically defined to use a particular SAN type, can result in bypassing name-constrained intermediates. Node.js &lt; 12.22.9, &lt; 14.18.3, &lt; 16.13.2, and &lt; 17.3.1 was accepting URI SAN types, which PKIs are often not defined to use. Additionally, when a protocol allows URI SANs, Node.js did not match the URI correctly. Versions of Node.js with the fix for this disable the URI SAN type when checking a certificate against a hostname. This behavior can be reverted through the --security-revert command-line option.</p>   |
| Node.js | 20.17.0 | CVE-2021-44532 | MEDIUM             | 5.3        | <p>Node.js &lt; 12.22.9, &lt; 14.18.3, &lt; 16.13.2, and &lt; 17.3.1 converts SANs (Subject Alternative Names) to a string format. It uses this string to check peer certificates against hostnames when validating connections. The string format was subject to an injection vulnerability when name constraints were used within a certificate chain, allowing the bypass of these name constraints. Versions of Node.js with the fix for this escape SANs containing the problematic characters in order to prevent the injection. This behavior can be reverted through the --security-revert command-line option.</p>   |

|         |         |                |                  |            |  |
|---------|---------|----------------|------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-44533 | MEDIUM           | 5.3        | Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 did not handle multi-value Relative Distinguished Names correctly. Attackers could craft certificate subjects containing a single-value Relative Distinguished Name that would be interpreted as a multi-value Relative Distinguished Name, for example, in order to inject a Common Name that would allow bypassing the certificate subject verification. Affected versions of Node.js that do not accept multi-value Relative Distinguished Names and are thus not vulnerable to such attacks themselves. However, third-party code that uses node's ambiguous presentation of certificate subjects may be vulnerable. |
| Node.js | 20.17.0 | CVE-2021-46708 | MEDIUM           | 6.1        | The swagger-ui-dist package before 4.1.3 for Node.js could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim.  |
| Node.js | 20.17.0 | CVE-2022-29080 | CRITICAL         | 9.8        | The npm-dependency-versions package through 0.3.0 for Node.js allows command injection if an attacker is able to call dependencyVersions with a JSON object in which pkgs is a key, and there are shell metacharacters in a value.   |
| Node.js | 20.17.0 | CVE-2022-29078 | CRITICAL         | 9.8        | The ejs (aka Embedded JavaScript templates) package 3.1.6 for Node.js allows server-side template injection in settings[view options][outputFunctionName]. This is parsed as an internal option, and overwrites the outputFunctionName option with an arbitrary OS command (which is executed upon template compilation).  |
| Node.js | 20.17.0 | CVE-2022-30241 | MEDIUM           | 6.1        | The jquery.json-viewer library through 1.4.0 for Node.js does not properly escape characters such as < in a JSON object, as demonstrated by a SCRIPT element.  |
| Node.js | 20.17.0 | CVE-2022-29166 | ['HIGH', 'HIGH'] | [8.0, 8.8] | matrix-appservice-irc is a Node.js IRC bridge for Matrix. The vulnerability in node-irc allows an attacker to manipulate a Matrix user into executing IRC commands by having them reply to a maliciously crafted message. The vulnerability has been patched in matrix-appservice-irc 0.33.2. Refrain from replying to messages from untrusted participants in IRC-bridged Matrix rooms. There are no known workarounds for this issue.  |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-29256 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.7] | sharp is an application for Node.js image processing. Prior to version 0.30.5, there is a possible vulnerability in logic that is run only at `npm install` time when installing versions of `sharp` prior to the latest v0.30.5. If an attacker has the ability to set the value of the `PKG_CONFIG_PATH` environment variable in a build environment then they might be able to use this to inject an arbitrary command at `npm install` time. This is not part of any runtime code, does not affect Windows users at all, and is unlikely to affect anyone that already cares about the security of their build environment. This problem is fixed in version 0.30.5. |
| Node.js | 20.17.0 | CVE-2021-34080 | CRITICAL             | 9.8        | OS Command Injection vulnerability in es128 ssl-utils 1.0.0 for Node.js allows attackers to execute arbitrary commands via unsanitized shell metacharacters provided to the createCertRequest() and the createCert() functions.  |
| Node.js | 20.17.0 | CVE-2021-34082 | CRITICAL             | 9.8        | OS Command Injection vulnerability in allenhwkim proctree through 0.1.1 and commit 0ac10ae575459457838f14e21d5996f2fa5c7593 for Node.js, allows attackers to execute arbitrary commands via the fix function.  |
| Node.js | 20.17.0 | CVE-2021-34083 | HIGH                 | 8.1        | Google-it is a Node.js package which allows its users to send search queries to Google and receive the results in a JSON format. When using the 'Open in browser' option in versions up to 1.6.2, google-it will unsafely concat the result's link retrieved from google to a shell command, potentially exposing the server to RCE.   |
| Node.js | 20.17.0 | CVE-2021-34084 | CRITICAL             | 9.8        | OS command injection vulnerability in Turistforeningen node-s3-uploader through 2.0.3 for Node.js allows attackers to execute arbitrary commands via the metadata() function.  |
| Node.js | 20.17.0 | CVE-2022-29244 | ['HIGH', 'HIGH']     | [7.5, 7.5] | npm pack ignores root-level .gitignore and .npmignore file exclusion directives when run in a workspace or with a workspace flag (ie. `--workspaces`, `--workspace=<name>`). Anyone who has run `npm pack` or `npm publish` inside a workspace, as of v7.9.0 and v7.13.0 respectively, may be affected and have published files into the npm registry they did not intend to include. Users should upgrade to the latest, patched version of npm v8.11.0, run: npm i -g npm@latest . Node.js versions v16.15.1, v17.19.1, and v18.3.0 include the patched v8.11.0 version of npm.  |

|         |         |                |                     |            |   |
|---------|---------|----------------|---------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-29247 | ['LOW', 'CRITICAL'] | [2.2, 9.8] | <p>Electron is a framework for writing cross-platform desktop applications using JavaScript (JS), HTML, and CSS. A vulnerability in versions prior to 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 allows a renderer with JS execution to obtain access to a new renderer process with `nodeIntegrationInSubFrames` enabled which in turn allows effective access to `ipcRenderer`. The `nodeIntegrationInSubFrames` option does not implicitly grant Node.js access. Rather, it depends on the existing sandbox setting. If an application is sandboxed, then `nodeIntegrationInSubFrames` just gives access to the sandboxed renderer APIs, which include `ipcRenderer`. If the application then additionally exposes IPC messages without IPC `senderFrame` validation that perform privileged actions or return confidential data this access to `ipcRenderer` can in turn compromise your application / user even with the sandbox enabled. Electron versions 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 contain a fix for this issue. ...</p> |
| Node.js | 20.17.0 | CVE-2022-31083 | ['HIGH', 'HIGH']    | [8.6, 7.5] | <p>Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 4.10.11 and 5.2.2, the certificate in the Parse Server Apple Game Center auth adapter not validated. As a result, authentication could potentially be bypassed by making a fake certificate accessible via certain Apple domains and providing the URL to that certificate in an authData object. Versions 4.0.11 and 5.2.2 prevent this by introducing a new `rootCertificateUrl` property to the Parse Server Apple Game Center auth adapter which takes the URL to the root certificate of Apple's Game Center authentication certificate. If no value is set, the `rootCertificateUrl` property defaults to the URL of the current root certificate as of May 27, 2022. Keep in mind that the root certificate can change at any time and that it is the developer's responsibility to keep the root certificate URL up-to-date when using the Parse Server Apple Game Center auth adapter. There are n...</p> |
| Node.js | 20.17.0 | CVE-2022-33987 | MEDIUM              | 5.3        | <p>The got package before 12.1.0 (also fixed in 11.8.5) for Node.js allows a redirect to a UNIX socket.</p>   |

|         |         |                |                  |            |  |
|---------|---------|----------------|------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-31089 | ['HIGH', 'HIGH'] | [7.5, 7.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In affected versions certain types of invalid files requests are not handled properly and can crash the server. If you are running multiple Parse Server instances in a cluster, the availability impact may be low; if you are running Parse Server as single instance without redundancy, the availability impact may be high. This issue has been addressed in versions 4.10.12 and 5.2.3. Users are advised to upgrade. There are no known workarounds for this issue. |
| Node.js | 20.17.0 | CVE-2022-31112 | ['HIGH', 'HIGH'] | [8.2, 8.2] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In affected versions parse Server LiveQuery does not remove protected fields in classes, passing them to the client. The LiveQueryController now removes protected fields from the client response. Users are advised to upgrade. Users unable to upgrade should use <code>Parse.Cloud.afterLiveQueryEvent</code> to manually remove protected fields.   |
| Node.js | 20.17.0 | CVE-2022-32212 | HIGH             | 8.1        | A OS Command Injection vulnerability exists in Node.js versions <14.20.0, <16.20.0, <18.5.0 due to an insufficient <code>IsAllowedHost</code> check that can easily be bypassed because <code>IsIPAddress</code> does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.  |
| Node.js | 20.17.0 | CVE-2022-32213 | MEDIUM           | 6.5        | The <code>Http</code> parser <v14.20.1, <v16.17.1 and <v18.9.1 in the <code>http</code> module in Node.js does not correctly parse and validate Transfer-Encoding headers and can lead to HTTP Request Smuggling (HRS).  |
| Node.js | 20.17.0 | CVE-2022-32214 | MEDIUM           | 6.5        | The <code>Http</code> parser <v14.20.1, <v16.17.1 and <v18.9.1 in the <code>http</code> module in Node.js does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS).   |
| Node.js | 20.17.0 | CVE-2022-32215 | MEDIUM           | 6.5        | The <code>Http</code> parser <v14.20.1, <v16.17.1 and <v18.9.1 in the <code>http</code> module in Node.js does not correctly handle multi-line Transfer-Encoding headers. This can lead to HTTP Request Smuggling (HRS).   |
| Node.js | 20.17.0 | CVE-2022-32222 | MEDIUM           | 5.3        | A cryptographic vulnerability exists on Node.js on linux in versions of 18.x prior to 18.40.0 which allowed a default path for <code>openssl.cnf</code> that might be accessible under some circumstances to a non-admin user instead of <code>/etc/ssl</code> as was the case in versions prior to the upgrade to OpenSSL 3.  |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-32223 | HIGH                     | 7.3        | Node.js is vulnerable to Hijack Execution Flow: DLL Hijacking under certain conditions on Windows platforms. This vulnerability can be exploited if the victim has the following dependencies on a Windows machine: * OpenSSL has been installed and <code>C:\Program Files\Common Files\SSL\openssl.cnf</code> exists. Whenever the above conditions are present, <code>node.exe</code> will search for <code>providers.dll</code> in the current user directory. After that, <code>node.exe</code> will try to search for <code>providers.dll</code> by the DLL Search Order in Windows. It is possible for an attacker to place the malicious file <code>providers.dll</code> under a variety of paths and exploit this vulnerability.  |
| Node.js | 20.17.0 | CVE-2022-31150 | ['MEDIUM', 'MEDIUM']     | [5.3, 6.5] | undici is an HTTP/1.1 client, written from scratch for Node.js. It is possible to inject CRLF sequences into request headers in undici in versions less than 5.7.1. A fix was released in version 5.8.0. Sanitizing all HTTP headers from untrusted sources to eliminate <code>\r\n</code> is a workaround for this issue.   |
| Node.js | 20.17.0 | CVE-2022-36313 | MEDIUM                   | 5.5        | An issue was discovered in the file-type package before 16.5.4 and 17.x before 17.1.3 for Node.js. A malformed MKV file could cause the file type detector to get caught in an infinite loop. This would make the application become unresponsive and could be used to cause a DoS attack.   |
| Node.js | 20.17.0 | CVE-2022-31183 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.8] | fs2 is a compositional, streaming I/O library for Scala. When establishing a server-mode <code>TLSSocket</code> using <code>fs2-io</code> on Node.js, the parameter <code>requestCert = true</code> is ignored, peer certificate verification is skipped, and the connection proceeds. The vulnerability is limited to: 1. <code>fs2-io</code> running on Node.js. The JVM TLS implementation is completely independent. 2. <code>TLSSocket</code> 's in server-mode. Client-mode <code>TLSSocket</code> 's are implemented via a different API. 3. mTLS as enabled via <code>requestCert = true</code> in <code>TLSPParameters</code> . The default setting is <code>false</code> for server-mode <code>TLSSocket</code> 's. It was introduced with the initial Node.js implementation of <code>fs2-io</code> in 3.1.0. A patch is released in v3.2.11. The <code>requestCert = true</code> parameter is respected and the peer certificate is verified. If verification fails, a <code>SSLException</code> is raised. If using an unpatched version on Node.js, do not use a server-mode <code>TLSSocket</code> with <code>requestCert = true</code> to establish a mTLS connection. |

|         |         |                |                        |            |   |
|---------|---------|----------------|------------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-35949 | ['MEDIUM', 'CRITICAL'] | [5.3, 9.8] | <p>undici is an HTTP/1.1 client, written from scratch for Node.js. `undici` is vulnerable to SSRF (Server-side Request Forgery) when an application takes in <b>user input</b> into the `path/pathname` option of `undici.request`. If a user specifies a URL such as `http://127.0.0.1` or `//127.0.0.1` ```js const undici = require("undici") undici.request({origin: "http://example.com", pathname: "//127.0.0.1"}) ``` Instead of processing the request as `http://example.org/127.0.0.1` (or `http://example.org/http://127.0.0.1` when `http://127.0.0.1` is used), it actually processes the request as `http://127.0.0.1/` and sends it to `http://127.0.0.1`. If a developer passes in user input into `path` parameter of `undici.request`, it can result in an <b>_SSRF_</b> as they will assume that the hostname cannot change, when in actual fact it can change because the specified path parameter is combined with the base URL. This issue was fixed in `undici@5.8.1`. The best workaround is to validate user input before...</p> |
| Node.js | 20.17.0 | CVE-2022-35948 | ['MEDIUM', 'MEDIUM']   | [5.3, 5.3] | <p>undici is an HTTP/1.1 client, written from scratch for Node.js. `&lt; undici@5.8.0` users are vulnerable to <b>_CRLF Injection_</b> on headers when using unsanitized input as request headers, more specifically, inside the `content-type` header. Example: ``` import { request } from 'undici' const unsanitizedContentTypeInput = 'application/json\r\n\r\nGET /foo2 HTTP/1.1' await request('http://localhost:3000, { method: 'GET', headers: { 'content-type': unsanitizedContentTypeInput }, }) ``` The above snippet will perform two requests in a single `request` API call: 1) `http://localhost:3000/` 2) `http://localhost:3000/foo2` This issue was patched in Undici v5.8.1. Sanitize input when sending content-type headers using user input as a workaround.</p>  |

|         |         |                |                          |            |   |
|---------|---------|----------------|--------------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-36045 | ['CRITICAL', 'CRITICAL'] | [9.0, 9.8] | NodeBB Forum Software is powered by Node.js and supports either Redis, MongoDB, or a PostgreSQL database. It utilizes web sockets for instant interactions and real-time notifications. <code>utils.generateUUID</code> , a helper function available in essentially all versions of NodeBB (as far back as v1.0.1 and potentially earlier) used a cryptographically insecure Pseudo-random number generator ( <code>Math.random()</code> ), which meant that a specially crafted script combined with multiple invocations of the password reset functionality could enable an attacker to correctly calculate the reset code for an account they do not have access to. This vulnerability impacts all installations of NodeBB. The vulnerability allows for an attacker to take over any account without the involvement of the victim, and as such, the remediation should be applied immediately (either via NodeBB upgrade or cherry-pick of the specific changeset. The vulnerability has been patched in version 2.x and 1.19.x. There is no known wor... |
| Node.js | 20.17.0 | CVE-2022-36046 | ['MEDIUM', 'MEDIUM']     | [5.3, 5.3] | Next.js is a React framework that can provide building blocks to create web applications. All of the following must be true to be affected by this CVE: Next.js version 12.2.3, Node.js version above v15.0.0 being used with strict <code>unhandledRejection</code> exiting AND using next start or a [custom server](https://nextjs.org/docs/advanced-features/custom-server). Deployments on Vercel ([vercel.com](https://vercel.com/)) are not affected along with similar environments where <code>next-server</code> isn't being shared across requests.  |
| Node.js | 20.17.0 | CVE-2022-36076 | ['HIGH', 'HIGH']         | [8.8, 7.5] | NodeBB Forum Software is powered by Node.js and supports either Redis, MongoDB, or a PostgreSQL database. Due to an unnecessarily strict conditional in the code handling the first step of the SSO process, the pre-existing logic that added (and later checked) a nonce was inadvertently rendered opt-in instead of opt-out. This re-exposed a vulnerability in that a specially crafted Man-in-the-Middle (MITM) attack could theoretically take over another user account during the single sign-on process. The issue has been fully patched in version 1.17.2.  |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-36079 | ['HIGH', 'HIGH']     | [8.6, 7.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Internal fields (keys used internally by Parse Server, prefixed by `_`) and protected fields (user defined) can be used as query constraints. Internal and protected fields are removed by Parse Server and are only returned to the client using a valid master key. However, using query constraints, these fields can be guessed by enumerating until Parse Server, prior to versions 4.10.14 or 5.2.5, returns a response object. The patch available in versions 4.10.14 and 5.2.5 requires the maser key to use internal and protected fields as query constraints. As a workaround, implement a Parse Cloud Trigger `beforeFind` and manually remove the query constraints.   |
| Node.js | 20.17.0 | CVE-2022-36083 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | JOSE is "JSON Web Almost Everything" - JWA, JWS, JWE, JWT, JWK, JWKS with no dependencies using runtime's native crypto in Node.js, Browser, Cloudflare Workers, Electron, and Deno. The PBKDF2-based JWE key management algorithms expect a JOSE Header Parameter named `p2c` PBES2 Count, which determines how many PBKDF2 iterations must be executed in order to derive a CEK wrapping key. The purpose of this parameter is to intentionally slow down the key derivation function in order to make password brute-force and dictionary attacks more expensive. This makes the PBES2 algorithms unsuitable for situations where the JWE is coming from an untrusted source: an adversary can intentionally pick an extremely high PBES2 Count value, that will initiate a CPU-bound computation that may take an unreasonable amount of time to finish. Under certain conditions, it is possible to have the user's environment consume unreasonable amount of CPU time. The impact is limited only to users utilizing the JWE d... |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-39202 | ['MEDIUM', 'MEDIUM'] | [4.3, 6.3] | matrix-appservice-irc is an open source Node.js IRC bridge for Matrix. The Internet Relay Chat (IRC) protocol allows you to specify multiple modes in a single mode command. Due to a bug in the underlying matrix-org/node-irc library, affected versions of matrix-appservice-irc perform parsing of such modes incorrectly, potentially resulting in the wrong user being given permissions. Mode commands can only be executed by privileged users, so this can only be abused if an operator is tricked into running the command on behalf of an attacker. The vulnerability has been patched in matrix-appservice-irc 0.35.0. As a workaround users should refrain from entering mode commands suggested by untrusted users. Avoid using multiple modes in a single command.  |
| Node.js | 20.17.0 | CVE-2022-39203 | ['HIGH', 'HIGH']     | [8.8, 8.8] | matrix-appservice-irc is an open source Node.js IRC bridge for Matrix. Attackers can specify a specific string of characters, which would confuse the bridge into combining an attacker-owned channel and an existing channel, allowing them to grant themselves permissions in the channel. The vulnerability has been patched in matrix-appservice-irc 0.35.0. As a workaround operators may disable dynamic channel joining via `dynamicChannels.enabled` to prevent users from joining new channels, which prevents any new channels being bridged outside of what is already bridged, and what is specified in the config.   |
| Node.js | 20.17.0 | CVE-2022-39225 | ['MEDIUM', 'LOW']    | [4.3, 3.1] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.15, or 5.0.0 and above prior to 5.2.6, a user can write to the session object of another user if the session object ID is known. For example, an attacker can assign the session object to their own user by writing to the `user` field and then read any custom fields of that session object. Note that assigning a session to another user does not usually change the privileges of either of the two users, and a user cannot assign their own session to another user. This issue is patched in version 4.10.15 and above, and 5.2.6 and above. To mitigate this issue in unpatched versions add a `beforeSave` trigger to the `_Session` class and prevent writing if the requesting user is different from the user in the session object. |

|         |         |                |                    |            |   |
|---------|---------|----------------|--------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-39231 | ['LOW', 'LOW']     | [3.7, 3.7] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.16, or from 5.0.0 to 5.2.6, validation of the authentication adapter app ID for <code>_Facebook_</code> and <code>_Spotify_</code> may be circumvented. Configurations which allow users to authenticate using the Parse Server authentication adapter where <code>`applds`</code> is set as a string instead of an array of strings authenticate requests from an app with a different app ID than the one specified in the <code>`applds`</code> configuration. For this vulnerability to be exploited, an attacker needs to be assigned an app ID by the authentication provider which is a sub-set of the server-side configured app ID. This issue is patched in versions 4.10.16 and 5.2.7. There are no known workarounds. |
| Node.js | 20.17.0 | CVE-2022-41340 | HIGH               | 7.5        | The <code>secp256k1-js</code> package before 1.1.0 for Node.js implements ECDSA without required <code>r</code> and <code>s</code> validation, leading to signature forgery.  |
| Node.js | 20.17.0 | CVE-2022-39287 | ['HIGH', 'MEDIUM'] | [8.1, 6.5] | <code>tiny-csrf</code> is a Node.js cross site request forgery (CSRF) protection middleware. In versions prior to 1.1.0 cookies were not encrypted and thus CSRF tokens were transmitted in the clear. This issue has been addressed in commit <code>`8eead6d`</code> and the patch will be included in version 1.1.0. Users are advised to upgrade. There are no known workarounds for this issue.   |
| Node.js | 20.17.0 | CVE-2022-39288 | ['HIGH', 'HIGH']   | [7.5, 7.5] | <code>fastify</code> is a fast and low overhead web framework, for Node.js. Affected versions of <code>fastify</code> are subject to a denial of service via malicious use of the Content-Type header. An attacker can send an invalid Content-Type header that can cause the application to crash. This issue has been addressed in commit <code>`fbb07e8d`</code> and will be included in release version 4.8.1. Users are advised to upgrade. Users unable to upgrade may manually filter out http content with malicious Content-Type headers.  |
| Node.js | 20.17.0 | CVE-2022-37616 | CRITICAL           | 9.8        | A prototype pollution vulnerability exists in the function <code>copy</code> in <code>dom.js</code> in the <code>xmldom</code> (published as <code>@xmldom/xmldom</code> ) package before 0.8.3 for Node.js via the <code>p</code> variable. NOTE: the vendor states "we are in the process of marking this report as invalid"; however, some third parties takes the position that "A prototype injection/Prototype pollution is not just when global objects are polluted with recursive merge or deep cloning but also when a target object is polluted."  |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-39299 | ['HIGH', 'HIGH']         | [7.4, 8.1] | Passport-SAML is a SAML 2.0 authentication provider for Passport, the Node.js authentication library. A remote attacker may be able to bypass SAML authentication on a website using passport-saml. A successful attack requires that the attacker is in possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to passport-saml version 3.2.2 or newer. The issue was also present in the beta releases of `node-saml` before version 4.0.0-beta.5. If you cannot upgrade, disabling SAML authentication may be done as a workaround. |
| Node.js | 20.17.0 | CVE-2022-39313 | ['HIGH', 'HIGH']         | [7.5, 7.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.17, and prior to 5.2.8 on the 5.x branch, crash when a file download request is received with an invalid byte range, resulting in a Denial of Service. This issue has been patched in versions 4.10.17, and 5.2.8. There are no known workarounds.  |
| Node.js | 20.17.0 | CVE-2022-39322 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.8] | @keystone-6/core is a core package for Keystone 6, a content management system for Node.js. Starting with version 2.2.0 and prior to version 2.3.1, users who expected their `multiselect` fields to use the field-level access control - if configured - are vulnerable to their field-level access control not being used. List-level access control is not affected. Field-level access control for fields other than `multiselect` are not affected. Version 2.3.1 contains a fix for this issue. As a workaround, stop using the `multiselect` field.   |

|         |         |                |                          |            |   |
|---------|---------|----------------|--------------------------|------------|---|
| Node.js | 20.17.0 | CVE-2022-39382 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | Keystone is a headless CMS for Node.js built with GraphQL and React. `@keystone-6/core@3.0.0    3.0.1` users that use `NODE_ENV` to trigger security-sensitive functionality in their production builds are vulnerable to `NODE_ENV` being inlined to `"development"` for user code, irrespective of what your environment variables. If you do not use `NODE_ENV` in your user code to trigger security-sensitive functionality, you are not impacted by this vulnerability. Any dependencies that use `NODE_ENV` to trigger particular behaviors (optimizations, security or otherwise) should still respect your environment's configured `NODE_ENV` variable. The application's dependencies, as found in `node_modules` (including `@keystone-6/core`), are typically not compiled as part of this process, and thus should be unaffected. We have tested this assumption by verifying that `NODE_ENV=production yarn keystone start` still uses secure cookies when using `statelessSessions`. This vulnerability has been f... |
| Node.js | 20.17.0 | CVE-2022-39396 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.18, and prior to 5.3.1 on the 5.X branch, are vulnerable to Remote Code Execution via prototype pollution. An attacker can use this prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. This issue is patched in version 5.3.1 and in 4.10.18. There are no known workarounds.  |
| Node.js | 20.17.0 | CVE-2022-41879 | ['HIGH', 'CRITICAL']     | [7.2, 9.8] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.3 or 4.10.20, a compromised Parse Server Cloud Code Webhook target endpoint allows an attacker to use prototype pollution to bypass the Parse Server `requestKeywordDenylist` option. This issue has been patched in versions 5.3.3 and 4.10.20. There are no known workarounds.   |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-41878 | ['HIGH', 'CRITICAL']     | [7.2, 9.8] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.2 or 4.10.19, keywords that are specified in the Parse Server option `requestKeywordDenylist` can be injected via Cloud Code Webhooks or Triggers. This will result in the keyword being saved to the database, bypassing the `requestKeywordDenylist` option. This issue is fixed in versions 4.10.19, and 5.3.2. If upgrade is not possible, the following Workarounds may be applied: Configure your firewall to only allow trusted servers to make request to the Parse Server Cloud Code Webhooks API, or block the API completely if you are not using the feature. |
| Node.js | 20.17.0 | CVE-2022-41940 | ['HIGH', 'MEDIUM']       | [7.1, 6.5] | Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the engine.io package, including those who uses depending packages like socket.io. There is no known workaround except upgrading to a safe version. There are patches for this issue released in versions 3.6.1 and 6.2.1.   |
| Node.js | 20.17.0 | CVE-2022-46164 | ['CRITICAL', 'CRITICAL'] | [9.4, 9.8] | NodeBB is an open source Node.js based forum software. Due to a plain object with a prototype being used in socket.io message handling a specially crafted payload can be used to impersonate other users and takeover accounts. This vulnerability has been patched in version 2.6.1. Users are advised to upgrade. Users unable to upgrade may cherry-pick commit `48d143921753914da45926cca6370a92ed0c46b8` into their codebase to patch the exploit.   |
| Node.js | 20.17.0 | CVE-2022-35255 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.1] | A weak randomness in WebCrypto keygen vulnerability exists in Node.js 18 due to a change with EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. There are two problems with this: 1) It does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail. 2) The random data returned by EntropySource() may not be cryptographically strong and therefore not suitable as keying material.   |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2022-43548 | ['HIGH', 'HIGH']     | [8.1, 8.1] | A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient <code>IsAllowedHost</code> check that can easily be bypassed because <code>IsIPAddress</code> does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks. The fix for this issue in <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212</a> was incomplete and this new CVE is to complete the fix.  |
| Node.js | 20.17.0 | CVE-2021-35065 | ['HIGH', 'HIGH']     | [7.5, 7.5] | The <code>glob-parent</code> package before 6.0.1 for Node.js allows ReDoS (regular expression denial of service) attacks against the enclosure regular expression.  |
| Node.js | 20.17.0 | CVE-2023-22474 | ['HIGH', 'HIGH']     | [8.7, 8.1] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server uses the request header <code>`x-forwarded-for`</code> to determine the client IP address. If Parse Server doesn't run behind a proxy server, then a client can set this header and Parse Server will trust the value of the header. The incorrect client IP address will be used by various features in Parse Server. This allows to circumvent the security mechanism of the Parse Server option <code>`masterKeyIps`</code> by setting an allowed IP address as the <code>`x-forwarded-for`</code> header value. This issue has been patched in version 5.4.1. The mechanism to determine the client IP address has been rewritten. The correct IP address determination now requires to set the Parse Server option <code>`trustProxy`</code> . |
| Node.js | 20.17.0 | CVE-2023-23936 | ['MEDIUM', 'MEDIUM'] | [6.5, 5.4] | Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect <code>`host`</code> HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the <code>`headers.host`</code> string before passing to undici.  |
| Node.js | 20.17.0 | CVE-2023-24807 | ['HIGH', 'HIGH']     | [7.5, 7.5] | Undici is an HTTP/1.1 client for Node.js. Prior to version 5.19.1, the <code>`Headers.set()`</code> and <code>`Headers.append()`</code> methods are vulnerable to Regular Expression Denial of Service (ReDoS) attacks when untrusted values are passed into the functions. This is due to the inefficient regular expression used to normalize the values in the <code>`headerValueNormalize()`</code> utility function. This vulnerability was patched in v5.19.1. No known workarounds are available.   |

|         |         |                |                          |             |  |
|---------|---------|----------------|--------------------------|-------------|--|
| Node.js | 20.17.0 | CVE-2023-25653 | ['HIGH', 'HIGH']         | [7.5, 7.5]  | node-jose is a JavaScript implementation of the JSON Object Signing and Encryption (JOSE) for web browsers and node.js-based servers. Prior to version 2.2.0, when using the non-default "fallback" crypto back-end, ECC operations in `node-jose` can trigger a Denial-of-Service (DoS) condition, due to a possible infinite loop in an internal calculation. For some ECC operations, this condition is triggered randomly; for others, it can be triggered by malicious input. The issue has been patched in version 2.2.0. Since this issue is only present in the "fallback" crypto implementation, it can be avoided by ensuring that either WebCrypto or the Node `crypto` module is available in the JS environment where `node-jose` is being run. |
| Node.js | 20.17.0 | CVE-2023-25813 | ['CRITICAL', 'CRITICAL'] | [10.0, 9.8] | Sequelize is a Node.js ORM tool. In versions prior to 6.19.1 a SQL injection exploit exists related to replacements. Parameters which are passed through replacements are not properly escaped which can lead to arbitrary SQL injection depending on the specific queries in use. The issue has been fixed in Sequelize 6.19.1. Users are advised to upgrade. Users unable to upgrade should not use the `replacements` and the `where` option in the same query.   |
| Node.js | 20.17.0 | CVE-2023-23918 | ['HIGH', 'HIGH']         | [7.5, 7.5]  | A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions ( <a href="https://nodejs.org/api/permissions.html">https://nodejs.org/api/permissions.html</a> ) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy.   |
| Node.js | 20.17.0 | CVE-2023-23919 | ['HIGH', 'HIGH']         | [7.5, 7.5]  | A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service.   |
| Node.js | 20.17.0 | CVE-2023-23920 | ['MEDIUM', 'MEDIUM']     | [4.2, 4.2]  | An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges.  |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2023-28155 | MEDIUM                   | 6.1        | The Request package through 2.88.1 for Node.js allows a bypass of SSRF mitigations via an attacker-controller server that does a cross-protocol redirect (HTTP to HTTPS, or HTTPS to HTTP).<br>NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  |
| Node.js | 20.17.0 | CVE-2018-25083 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | The pullit package before 1.4.0 for Node.js allows OS Command Injection because eval is used on an attacker-supplied Git branch name.  |
| Node.js | 20.17.0 | CVE-2022-2237  | ['MEDIUM', 'MEDIUM']     | [6.1, 6.1] | A flaw was found in the Keycloak Node.js Adapter. This flaw allows an attacker to benefit from an Open Redirect vulnerability in the checkSso function.  |
| Node.js | 20.17.0 | CVE-2023-31125 | ['MEDIUM', 'MEDIUM']     | [6.5, 6.5] | Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. An uncaught exception vulnerability was introduced in version 5.1.0 and included in version 4.1.0 of the `socket.io` parent package. Older versions are not impacted. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the `engine.io` package, including those who use depending packages like `socket.io`. This issue was fixed in version 6.4.2 of Engine.IO. There is no known workaround except upgrading to a safe version. |
| Node.js | 20.17.0 | CVE-2023-27562 | ['MEDIUM', 'MEDIUM']     | [6.5, 6.5] | The n8n package 0.218.0 for Node.js allows Directory Traversal.  |
| Node.js | 20.17.0 | CVE-2023-27563 | ['HIGH', 'HIGH']         | [8.8, 8.8] | The n8n package 0.218.0 for Node.js allows Escalation of Privileges.   |
| Node.js | 20.17.0 | CVE-2023-27564 | ['HIGH', 'HIGH']         | [7.5, 7.5] | The n8n package 0.218.0 for Node.js allows Information Disclosure.   |
| Node.js | 20.17.0 | CVE-2023-26127 | ['HIGH', 'HIGH']         | [7.8, 7.8] | All versions of the package n158 are vulnerable to Command Injection due to improper input sanitization in the `module.exports` function.<br>**Note:** To execute the code snippet and potentially exploit the vulnerability, the attacker needs to have the ability to run Node.js code within the target environment. This typically requires some level of access to the system or application hosting the Node.js environment.   |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2023-26128 | ['HIGH', 'HIGH']     | [8.4, 7.8] | All versions of the package keep-module-latest are vulnerable to Command Injection due to missing input sanitization or other checks and sandboxes being employed to the installModule function.<br>**Note:** To execute the code snippet and potentially exploit the vulnerability, the attacker needs to have the ability to run Node.js code within the target environment. This typically requires some level of access to the system or application hosting the Node.js environment.   |
| Node.js | 20.17.0 | CVE-2023-26129 | ['HIGH', 'HIGH']     | [8.4, 7.8] | All versions of the package bwm-ng are vulnerable to Command Injection due to improper input sanitization in the 'check' function in the bwm-ng.js file.<br>**Note:** To execute the code snippet and potentially exploit the vulnerability, the attacker needs to have the ability to run Node.js code within the target environment. This typically requires some level of access to the system or application hosting the Node.js environment.   |
| Node.js | 20.17.0 | CVE-2023-32695 | ['HIGH', 'HIGH']     | [7.3, 7.5] | socket.io parser is a socket.io encoder and decoder written in JavaScript complying with version 5 of socket.io-protocol. A specially crafted Socket.IO packet can trigger an uncaught exception on the Socket.IO server, thus killing the Node.js process. A patch has been released in version 4.2.3.   |
| Node.js | 20.17.0 | CVE-2023-32689 | ['MEDIUM', 'MEDIUM'] | [6.3, 6.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 5.4.4 and 6.1.1 are vulnerable to a phishing attack vulnerability that involves a user uploading malicious files. A malicious user could upload an HTML file to Parse Server via its public API. That HTML file would then be accessible at the internet domain at which Parse Server is hosted. The URL of the the uploaded HTML could be shared for phishing attacks. The HTML page may seem legitimate because it is served under the internet domain where Parse Server is hosted, which may be the same as a company's official website domain. An additional security issue arises when the Parse JavaScript SDK is used. The SDK stores sessions in the internet browser's local storage, which usually restricts data access depending on the internet domain. A malicious HTML file could contain a script that retrieves the user's session token from local storage and then share it with the ... |
| Node.js | 20.17.0 | CVE-2020-36732 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | The crypto-js package before 3.2.1 for Node.js generates random numbers by concatenating the string "0." with an integer, which makes the output more predictable than necessary.   |

|         |         |                |                          |             |   |
|---------|---------|----------------|--------------------------|-------------|---|
| Node.js | 20.17.0 | CVE-2023-34247 | ['MEDIUM', 'MEDIUM']     | [6.1, 4.1]  | Keystone is a content management system for Node.JS. There is an open redirect in the `@keystone-6/auth` package versions 7.0.0 and prior, where the redirect leading `^` filter can be bypassed. Users may be redirected to domains other than the relative host, thereby it might be used by attackers to re-direct users to an unexpected location. To mitigate this issue, one may apply a patch from pull request 8626 or avoid using the `@keystone-6/auth` package.  |
| Node.js | 20.17.0 | CVE-2023-36475 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8]  | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 5.5.2 and 6.2.1, an attacker can use a prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. A patch is available in versions 5.5.2 and 6.2.1.   |
| Node.js | 20.17.0 | CVE-2023-30586 | ['HIGH', 'HIGH']         | [7.5, 7.5]  | A privilege escalation vulnerability exists in Node.js 20 that allowed loading arbitrary OpenSSL engines when the experimental permission model is enabled, which can bypass and/or disable the permission model. The attack complexity is high. However, the crypto.setEngine() API can be used to bypass the permission model when called with a compatible OpenSSL engine. The OpenSSL engine can, for example, disable the permission model in the host process by manipulating the process's stack memory to locate the permission model Permission::enabled_ in the host process's heap memory. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. |
| Node.js | 20.17.0 | CVE-2023-30589 | HIGH                     | 7.5         | The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20   |
| Node.js | 20.17.0 | CVE-2023-37466 | ['CRITICAL', 'CRITICAL'] | [9.8, 10.0] | vm2 is an advanced vm/sandbox for Node.js. The library contains critical security issues and should not be used for production. The maintenance of the project has been discontinued. In vm2 for versions up to 3.9.19, `Promise` handler sanitization can be bypassed with the `@@species` accessor property allowing attackers to escape the sandbox and run arbitrary code, potentially allowing remote code execution inside the context of vm2 sandbox.  |

|         |         |                |                          |             |  |
|---------|---------|----------------|--------------------------|-------------|--|
| Node.js | 20.17.0 | CVE-2023-37903 | ['CRITICAL', 'CRITICAL'] | [9.8, 10.0] | vm2 is an open source vm/sandbox for Node.js. In vm2 for versions up to and including 3.9.19, Node.js custom inspect function allows attackers to escape the sandbox and run arbitrary code. This may result in Remote Code Execution, assuming the attacker has arbitrary code execution primitive inside the context of vm2 sandbox. There are no patches and no known workarounds. Users are advised to find an alternative software.   |
| Node.js | 20.17.0 | CVE-2023-26045 | ['CRITICAL', 'CRITICAL'] | [10.0, 9.8] | NodeBB is Node.js based forum software. Starting in version 2.5.0 and prior to version 2.8.7, due to the use of the object destructuring assignment syntax in the user export code path, combined with a path traversal vulnerability, a specially crafted payload could invoke the user export logic to arbitrarily execute javascript files on the local disk. This issue is patched in version 2.8.7. As a workaround, site maintainers can cherry pick the fix into their codebase to patch the exploit. |
| Node.js | 20.17.0 | CVE-2023-38504 | ['HIGH', 'HIGH']         | [7.5, 7.5]  | Sails is a realtime MVC Framework for Node.js. In Sails apps prior to version 1.5.7,, an attacker can send a virtual request that will cause the node process to crash. This behavior was fixed in Sails v1.5.7. As a workaround, disable the sockets hook and remove the `sails.io.js` client.  |
| Node.js | 20.17.0 | CVE-2023-38690 | ['MEDIUM', 'CRITICAL']   | [5.8, 9.8]  | matrix-appservice-irc is a Node.js IRC bridge for Matrix. Prior to version 1.0.1, it is possible to craft a command with newlines which would not be properly parsed. This would mean you could pass a string of commands as a channel name, which would then be run by the IRC bridge bot. Versions 1.0.1 and above are patched. There are no robust workarounds to the bug. One may disable dynamic channels in the config to disable the most common execution method but others may exist.               |
| Node.js | 20.17.0 | CVE-2023-38700 | ['LOW', 'LOW']           | [3.5, 3.7]  | matrix-appservice-irc is a Node.js IRC bridge for Matrix. Prior to version 1.0.1, it was possible to craft an event such that it would leak part of a targeted message event from another bridged room. This required knowing an event ID to target. Version 1.0.1n fixes this issue. As a workaround, set the `matrixHandler.eventCacheSize` config value to `0`. This workaround may impact performance.   |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2023-39532 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | <p>SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no endowments can gain access to the surrounding host's dynamic import by using dynamic import after the spread operator, like <code>{...import(arbitraryModuleSpecifier)}</code>. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the applic...</p> |
| Node.js | 20.17.0 | CVE-2023-32003 | MEDIUM                   | 5.3        | <p><code>fs.mkdtemp()</code> and <code>fs.mkdtempSync()</code> can be used to bypass the permission model check using a path traversal attack. This flaw arises from a missing check in the <code>fs.mkdtemp()</code> API and the impact is a malicious actor could create an arbitrary directory. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.</p>   |
| Node.js | 20.17.0 | CVE-2023-32004 | ['HIGH', 'HIGH']         | [8.8, 8.8] | <p>A vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model. This flaw relates to improper handling of Buffers in file system APIs causing a traversal path to bypass when verifying file permissions. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.</p>   |
| Node.js | 20.17.0 | CVE-2023-32006 | ['HIGH', 'HIGH']         | [8.8, 8.8] | <p>The use of <code>module.constructor.createRequire()</code> can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x, and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.</p>   |

|         |         |                |                   |            |  |
|---------|---------|----------------|-------------------|------------|--|
| Node.js | 20.17.0 | CVE-2023-40027 | ['LOW', 'MEDIUM'] | [3.7, 5.3] | Keystone is an open source headless CMS for Node.js built with GraphQL and React. When <code>`ui.isAccessAllowed`</code> is set as <code>`undefined`</code> , the <code>`adminMeta`</code> GraphQL query is publicly accessible (no session required). This is different to the behaviour of the default AdminUI middleware, which by default will only be publicly accessible (no session required) if a <code>`session`</code> strategy is not defined. This vulnerability does not affect developers using the <code>`@keystone-6/auth`</code> package, or any users that have written their own <code>`ui.isAccessAllowed`</code> (that is to say, <code>`isAccessAllowed`</code> is not <code>`undefined`</code> ). This vulnerability does affect users who believed that their <code>`session`</code> strategy will, by default, enforce that <code>`adminMeta`</code> is inaccessible by the public in accordance with that strategy; akin to the behaviour of the AdminUI middleware. This vulnerability has been patched in <code>`@keystone-6/core`</code> version <code>`5.5.1`</code> . Users are advised to upgrade. Users unable to upgrade may opt to write their own <code>`isAccessA...</code> |
| Node.js | 20.17.0 | CVE-2023-32002 | CRITICAL          | 9.8        | The use of <code>`Module._load()`</code> can bypass the policy mechanism and require modules outside of the <code>policy.json</code> definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2023-32559 | HIGH              | 7.5        | A privilege escalation vulnerability exists in the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. The use of the deprecated API <code>`process.binding()`</code> can bypass the policy mechanism by requiring internal modules and eventually take advantage of <code>`process.binding('spawn_sync')`</code> run arbitrary code, outside of the limits defined in a <code>`policy.json`</code> file. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.   |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2021-32050 | ['MEDIUM', 'HIGH']       | [4.2, 7.5] | Some MongoDB Drivers may erroneously publish events containing authentication-related data to a command listener configured by an application. The published events may contain security-sensitive data when specific authentication-related commands are executed. Without due care, an application may inadvertently expose this sensitive information, e.g., by writing it to a log file. This issue only arises if an application enables the command listener feature (this is not enabled by default). This issue affects the MongoDB C Driver 1.0.0 prior to 1.17.7, MongoDB PHP Driver 1.0.0 prior to 1.9.2, MongoDB Swift Driver 1.0.0 prior to 1.1.1, MongoDB Node.js Driver 3.6 prior to 3.6.10, MongoDB Node.js Driver 4.0 prior to 4.17.0 and MongoDB Node.js Driver 5.0 prior to 5.8.0. This issue also affects users of the MongoDB C++ Driver dependent on the C driver 1.0.0 prior to 1.17.7 (C++ driver prior to 3.7.0). |
| Node.js | 20.17.0 | CVE-2023-32005 | ['MEDIUM', 'MEDIUM']     | [5.3, 5.3] | A vulnerability has been identified in Node.js version 20, affecting users of the experimental permission model when the --allow-fs-read flag is used with a non-* argument. This flaw arises from an inadequate permission model that fails to restrict file stats through the `fs.statfs` API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2023-32558 | HIGH                     | 7.5        | The use of the deprecated API `process.binding()` can bypass the permission model through path traversal. This vulnerability affects all users using the experimental permission model in Node.js 20.x. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2023-42810 | ['CRITICAL', 'CRITICAL'] | [9.8, 9.8] | systeminformation is a System Information Library for Node.JS. Versions 5.0.0 through 5.21.6 have a SSID Command Injection Vulnerability. The problem was fixed with a parameter check in version 5.21.7. As a workaround, check or sanitize parameter strings that are passed to `wifiConnections()`, `wifiNetworks()` (string only).   |

|         |         |                |                |            |   |
|---------|---------|----------------|----------------|------------|---|
| Node.js | 20.17.0 | CVE-2023-45143 | ['LOW', 'LOW'] | [3.9, 3.5] | Undici is an HTTP/1.1 client written from scratch for Node.js. Prior to version 5.26.2, Undici already cleared Authorization headers on cross-origin redirects, but did not clear `Cookie` headers. By design, `cookie` headers are forbidden request headers, disallowing them to be set in RequestInit.headers in browser environments. Since undici handles headers more liberally than the spec, there was a disconnect from the assumptions the spec made, and undici's implementation of fetch. As such this may lead to accidental leakage of cookie to a third-party site or a malicious attacker who can control the redirection target (ie. an open redirector) to leak the cookie to the third party site. This was patched in version 5.26.2. There are no known workarounds. |
| Node.js | 20.17.0 | CVE-2023-38552 | HIGH           | 7.5        | When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can intercept the operation and return a forged checksum to the node's policy implementation, thus effectively disabling the integrity check. Impacts: This vulnerability affects all users using the experimental policy mechanism in all active release lines: 18.x and, 20.x. Please note that at the time this CVE was issued, the policy mechanism is an experimental feature of Node.js.   |
| Node.js | 20.17.0 | CVE-2023-39331 | HIGH           | 7.5        | A previously disclosed vulnerability (CVE-2023-30584) was patched insufficiently in commit 205f1e6. The new path traversal vulnerability arises because the implementation does not protect itself against the application overwriting built-in utility functions with user-defined implementations. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2023-39332 | CRITICAL       | 9.8        | Various `node:fs` functions allow specifying paths as either strings or `Uint8Array` objects. In Node.js environments, the `Buffer` class extends the `Uint8Array` class. Node.js prevents path traversal through strings (see CVE-2023-30584) and `Buffer` objects (see CVE-2023-32004), but not through non-`Buffer` `Uint8Array` objects. This is distinct from CVE-2023-32004 which only referred to `Buffer` objects. However, the vulnerability follows the same pattern using `Uint8Array` instead of `Buffer`. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |

|         |         |                |                  |            |  |
|---------|---------|----------------|------------------|------------|--|
| Node.js | 20.17.0 | CVE-2023-46119 | ['HIGH', 'HIGH'] | [7.5, 7.5] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server crashes when uploading a file without extension. This vulnerability has been patched in versions 5.5.6 and 6.3.1.   |
| Node.js | 20.17.0 | CVE-2023-30581 | HIGH             | 7.5        | The use of <code>__proto__</code> in <code>process.mainModule.__proto__</code> . <code>require()</code> can bypass the policy mechanism and require modules outside of the <code>policy.json</code> definition. This vulnerability affects all users using the experimental policy mechanism in all active release lines: v16, v18 and, v20. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js  |
| Node.js | 20.17.0 | CVE-2023-30585 | HIGH             | 7.5        | A vulnerability has been identified in the Node.js (.msi version) installation process, specifically affecting Windows users who install Node.js using the .msi installer. This vulnerability emerges during the repair operation, where the "msiexec.exe" process, running under the NT AUTHORITY\SYSTEM context, attempts to read the %USERPROFILE% environment variable from the current user's registry. The issue arises when the path referenced by the %USERPROFILE% environment variable does not exist. In such cases, the "msiexec.exe" process attempts to create the specified path in an unsafe manner, potentially leading to the creation of arbitrary folders in arbitrary locations. The severity of this vulnerability is heightened by the fact that the %USERPROFILE% environment variable in the Windows registry can be modified by standard (or "non-privileged") users. Consequently, unprivileged actors, including malicious entities or trojans, can manipulate the environment variable key to deceive ... |
| Node.js | 20.17.0 | CVE-2023-30588 | MEDIUM           | 5.3        | When an invalid public key is used to create an x509 certificate using the <code>crypto.X509Certificate()</code> API a non-expect termination occurs making it susceptible to DoS attacks when the attacker could force interruptions of application processing, as the process terminates when accessing public key info of provided certificates from user code. The current context of the users will be gone, and that will cause a DoS scenario. This vulnerability affects all active Node.js versions v16, v18, and, v20.   |

|         |         |                |                    |            |  |
|---------|---------|----------------|--------------------|------------|--|
| Node.js | 20.17.0 | CVE-2023-49803 | ['HIGH', 'HIGH']   | [8.6, 7.5] | @koa/cors npm provides Cross-Origin Resource Sharing (CORS) for koa, a web framework for Node.js. Prior to version 5.0.0, the middleware operates in a way that if an allowed origin is not provided, it will return an `Access-Control-Allow-Origin` header with the value of the origin from the request. This behavior completely disables one of the most crucial elements of browsers - the Same Origin Policy (SOP), this could cause a very serious security threat to the users of this middleware. If such behavior is expected, for instance, when middleware is used exclusively for prototypes and not for production applications, it should be heavily emphasized in the documentation along with an indication of the risks associated with such behavior, as many users may not be aware of it. Version 5.0.0 fixes this vulnerability.  |
| Node.js | 20.17.0 | CVE-2023-50728 | ['MEDIUM', 'HIGH'] | [5.4, 7.5] | octokit/webhooks is a GitHub webhook events toolset for Node.js. Starting in 9.26.0 and prior to 9.26.3, 10.9.2, 11.1.2, and 12.0.4, there is a problem caused by an issue with error handling in the @octokit/webhooks library because the error can be undefined in some cases. The resulting request was found to cause an uncaught exception that ends the nodejs process. The bug is fixed in octokit/webhooks.js 9.26.3, 10.9.2, 11.1.2, and 12.0.4, app.js 14.02, octokit.js 3.1.2, and Protobot 12.3.3.  |
| Node.js | 20.17.0 | CVE-2023-48795 | MEDIUM             | 5.9        | The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before... |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2024-23340 | ['MEDIUM', 'MEDIUM'] | [5.3, 5.3] | @hono/node-server is an adapter that allows users to run Hono applications on Node.js. Since v1.3.0, @hono/node-server has used its own Request object with `url` behavior that is unexpected. In the standard API, if the URL contains `..`, here called "double dots", the URL string returned by Request will be in the resolved path. However, the `url` in @hono/node-server's Request as does not resolve double dots, so `http://localhost/static/.. /foo.txt` is returned. This causes vulnerabilities when using `serveStatic`. Modern web browsers and a latest `curl` command resolve double dots on the client side, so this issue doesn't affect those using either of those tools. However, problems may occur if accessed by a client that does not resolve them. Version 1.4.1 includes the change to fix this issue. As a workaround, don't use `serveStatic`.  |
| Node.js | 20.17.0 | CVE-2024-23743 | ['LOW', 'LOW']       | [3.3, 3.3] | Notion through 3.1.0 on macOS might allow code execution because of RunAsNode and enableNodeCliInspectArguments. NOTE: the vendor states "the attacker must launch the Notion Desktop application with nonstandard flags that turn the Electron-based application into a Node.js execution environment."   |
| Node.js | 20.17.0 | CVE-2023-42282 | CRITICAL             | 9.8        | The ip package before 1.1.9 for Node.js might allow SSRF because some IP addresses (such as 0x7f.1) are improperly categorized as globally routable via isPublic.  |
| Node.js | 20.17.0 | CVE-2024-24828 | ['MEDIUM', 'HIGH']   | [6.6, 7.8] | pkg is tool design to bundle Node.js projects into an executables. Any native code packages built by `pkg` are written to a hardcoded directory. On unix systems, this is `/tmp/pkg/*` which is a shared directory for all users on the same local system. There is no uniqueness to the package names within this directory, they are predictable. An attacker who has access to the same local system has the ability to replace the genuine executables in the shared directory with malicious executables of the same name. A user may then run the malicious executable without realising it has been modified. This package is deprecated. Therefore, there will not be a patch provided for this vulnerability. To check if your executable build by pkg depends on native code and is vulnerable, run the executable and check if `/tmp/pkg/` was created. Users should transition to actively maintained alternatives. We would recommend investigating Node.js 21's support for single executable applications. Given the... |

|         |         |                |                      |            |  |
|---------|---------|----------------|----------------------|------------|--|
| Node.js | 20.17.0 | CVE-2024-24750 | ['MEDIUM', 'MEDIUM'] | [6.5, 6.5] | Undici is an HTTP/1.1 client, written from scratch for Node.js. In affected versions calling <code>fetch(url)</code> and not consuming the incoming body ((or consuming it very slowing) will lead to a memory leak. This issue has been addressed in version 6.6.1. Users are advised to upgrade. Users unable to upgrade should make sure to always consume the incoming body.   |
| Node.js | 20.17.0 | CVE-2024-24758 | ['LOW', 'MEDIUM']    | [3.9, 4.5] | Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici already cleared Authorization headers on cross-origin redirects, but did not clear <code>Proxy-Authentication</code> headers. This issue has been patched in versions 5.28.3 and 6.6.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.  |
| Node.js | 20.17.0 | CVE-2024-21890 | MEDIUM               | 6.5        | The Node.js Permission Model does not clarify in the documentation that wildcards should be only used as the last character of a file path. For example: <code>--allow-fs-read=/home/node/.ssh/*.pub</code> will ignore <code>.pub</code> and give access to everything after <code>.ssh/</code> . This misleading documentation affects all users using the experimental permission model in Node.js 20 and Node.js 21. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. |
| Node.js | 20.17.0 | CVE-2024-21891 | HIGH                 | 8.8        | Node.js depends on multiple built-in utility functions to normalize paths provided to node:fs functions, which can be overwritten with user-defined implementations leading to filesystem permission model bypass through path traversal attack. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 21. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2024-21892 | HIGH                 | 7.8        | On Linux, Node.js ignores certain environment variables if those may have been set by an unprivileged user while the process is running with elevated privileges with the only exception of <code>CAP_NET_BIND_SERVICE</code> . Due to a bug in the implementation of this exception, Node.js incorrectly applies this exception even when certain other capabilities have been set. This allows unprivileged users to inject code that inherits the process's elevated privileges.  |

|         |         |                |          |      |   |
|---------|---------|----------------|----------|------|---|
| Node.js | 20.17.0 | CVE-2024-21896 | CRITICAL | 9.8  | The permission model protects itself against path traversal attacks by calling path.resolve() on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses Buffer.from() to obtain a Buffer from the result of path.resolve(). By monkey-patching Buffer internals, namely, Buffer.prototype.utf8Write, the application can modify the result of path.resolve(), which leads to a path traversal vulnerability. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 21. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. |
| Node.js | 20.17.0 | CVE-2024-22019 | HIGH     | 7.5  | A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, exploiting the lack of limitations on chunk extension bytes. The issue can cause CPU and network bandwidth exhaustion, bypassing standard safeguards like timeouts and body size limits.   |
| Node.js | 20.17.0 | CVE-2024-27298 | CRITICAL | 10.0 | parse-server is a Parse Server for Node.js / Express. This vulnerability allows SQL injection when Parse Server is configured to use the PostgreSQL database. The vulnerability has been fixed in 6.5.0 and 7.0.0-alpha.20.   |
| Node.js | 20.17.0 | CVE-2024-22017 | None     | None | setuid() does not affect libuv's internal io_uring operations if initialized before the call to setuid(). This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to setuid(). This vulnerability affects all users using version greater or equal than Node.js 18.18.0, Node.js 20.4.0 and Node.js 21.   |
| Node.js | 20.17.0 | CVE-2024-22025 | None     | None | A vulnerability in Node.js has been identified, allowing for a Denial of Service (DoS) attack through resource exhaustion when using the fetch() function to retrieve content from an untrusted URL. The vulnerability stems from the fact that the fetch() function in Node.js always decodes Brotli, making it possible for an attacker to cause resource exhaustion when fetching content from an untrusted URL. An attacker controlling the URL passed into fetch() can exploit this vulnerability to exhaust memory, potentially leading to process termination, depending on the system configuration.  |

|         |         |                |                  |            |  |
|---------|---------|----------------|------------------|------------|--|
| Node.js | 20.17.0 | CVE-2024-29027 | CRITICAL         | 9.0        | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 6.5.5 and 7.0.0-alpha.29, calling an invalid Parse Server Cloud Function name or Cloud Job name crashes the server and may allow for code injection, internal store manipulation or remote code execution. The patch in versions 6.5.5 and 7.0.0-alpha.29 added string sanitation for Cloud Function name and Cloud Job name. As a workaround, sanitize the Cloud Function name and Cloud Job name before it reaches Parse Server.   |
| Node.js | 20.17.0 | CVE-2024-27935 | ['HIGH', 'HIGH'] | [7.2, 8.3] | Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.35.1 and prior to version 1.36.3, a vulnerability in Deno's Node.js compatibility runtime allows for cross-session data contamination during simultaneous asynchronous reads from Node.js streams sourced from sockets or files. The issue arises from the re-use of a global buffer (BUF) in stream_wrap.ts used as a performance optimization to limit allocations during these asynchronous read operations. This can lead to data intended for one session being received by another session, potentially resulting in data corruption and unexpected behavior. This affects all users of Deno that use the node.js compatibility layer for network communication or other streams, including packages that may require node.js libraries indirectly. Version 1.36.3 contains a patch for this issue. |
| Node.js | 20.17.0 | CVE-2024-28863 | MEDIUM           | 6.5        | node-tar is a Tar for Node.js. node-tar prior to version 6.2.1 has no limit on the number of sub-folders created in the folder creation process. An attacker who generates a large number of sub-folders can consume memory on the system running node-tar and even crash the Node.js client within few seconds of running it using a path with too many sub-folders inside. Version 6.2.1 fixes this issue by preventing extraction in excessively deep sub-folders.  |

|         |         |                |                   |            |  |
|---------|---------|----------------|-------------------|------------|--|
| Node.js | 20.17.0 | CVE-2024-29042 | MEDIUM            | 5.3        | Translate is a package that allows users to convert text to different languages on Node.js and the browser. Prior to version 3.0.0, an attacker controlling the second variable of the `translate` function is able to perform a cache poisoning attack. They can change the outcome of translation requests made by subsequent users. The `opt.id` parameter allows the overwriting of the cache key. If an attacker sets the `id` variable to the cache key that would be generated by another user, they can choose the response that user gets served. Version 3.0.0 fixes this issue. |
| Node.js | 20.17.0 | CVE-2024-29900 | ['HIGH', 'HIGH']  | [7.5, 7.5] | Electron Packager bundles Electron-based application source code with a renamed Electron executable and supporting files into folders ready for distribution. A random segment of ~1-10kb of Node.js heap memory allocated either side of a known buffer will be leaked into the final executable. This memory _could_ contain sensitive information such as environment variables, secrets files, etc. This issue is patched in 18.3.1.   |
| Node.js | 20.17.0 | CVE-2024-30261 | ['LOW', 'LOW']    | [2.6, 3.5] | Undici is an HTTP/1.1 client, written from scratch for Node.js. An attacker can alter the `integrity` option passed to `fetch()`, allowing `fetch()` to accept requests as valid even if they have been tampered. This vulnerability was patched in version(s) 5.28.4 and 6.11.1.  |
| Node.js | 20.17.0 | CVE-2024-30260 | ['LOW', 'MEDIUM'] | [3.9, 4.3] | Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici cleared Authorization and Proxy-Authorization headers for `fetch()`, but did not clear them for `undici.request()`. This vulnerability was patched in version(s) 5.28.4 and 6.11.1.   |
| Node.js | 20.17.0 | CVE-2024-27983 | None              | None       | An attacker can make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside. It is possible to leave some data in nghttp2 memory after reset when headers with HTTP/2 CONTINUATION frame are sent to the server and then a TCP connection is abruptly closed by the client triggering the Http2Session destructor while header frames are still being processed (and stored in memory) causing a race condition.  |

|         |         |                |          |      |  |
|---------|---------|----------------|----------|------|--|
| Node.js | 20.17.0 | CVE-2024-32000 | MEDIUM   | 4.3  | matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. matrix-appservice-irc before version 2.0.0 can be exploited to leak the truncated body of a message if a malicious user sends a Matrix reply to an event ID they don't have access to. As a precondition to the attack, the malicious user needs to know the event ID of the message they want to leak, as well as to be joined to both the Matrix room and the IRC channel it is bridged to. The message reply containing the leaked message content is visible to IRC channel members when this happens. matrix-appservice-irc 2.0.0 checks whether the user has permission to view an event before constructing a reply. Administrators should upgrade to this version. It's possible to limit the amount of information leaked by setting a reply template that doesn't contain the original message. See these lines `601-604` in the configuration file linked.   |
| Node.js | 20.17.0 | CVE-2024-32652 | HIGH     | 7.5  | The adapter @hono/node-server allows you to run your Hono application on Node.js. Prior to 1.10.1, the application hangs when receiving a Host header with a value that `@hono/node-server` can't handle well. Invalid values are those that cannot be parsed by the `URL` as a hostname such as an empty string, slashes `/`, and other strings. The version 1.10.1 includes the fix for this issue.  |
| Node.js | 20.17.0 | CVE-2024-33883 | MEDIUM   | 4.0  | The ejs (aka Embedded JavaScript templates) package before 3.1.10 for Node.js lacks certain pollution protection.  |
| Node.js | 20.17.0 | CVE-2024-32962 | CRITICAL | 10.0 | xml-crypto is an xml digital signature and encryption library for Node.js. In affected versions the default configuration does not check authorization of the signer, it only checks the validity of the signature per section 3.2.2 of the w3 xmldsig-core-20080610 spec. As such, without additional validation steps, the default configuration allows a malicious actor to re-sign an XML document, place the certificate in a ` <keyinfo &gt;`="" &gt;`.="" (`publiccert`)="" (created="" `<keyinfo="" `xml-crypto`="" a="" an="" and="" any="" as="" atta...<="" attacker="" by="" can="" certificate="" checks.="" configured="" default="" digitally="" document="" document's="" element,="" even="" existing="" for="" generated="" if="" key="" library="" malicious="" modifying="" pass="" prefers="" private="" provided="" purposes.="" replacing="" result="" signature="" signed="" specific="" spoof="" td="" to="" trusts="" use="" validation="" verification="" via="" was="" with="" xml=""></keyinfo> |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2024-34347 | HIGH                 | 8.3        | @hoppscotch/cli is a CLI to run Hoppscotch Test Scripts in CI environments. Prior to 0.8.0, the @hoppscotch/js-sandbox package provides a Javascript sandbox that uses the Node.js vm module. However, the vm module is not safe for sandboxing untrusted Javascript code. This is because code inside the vm context can break out if it can get a hold of any reference to an object created outside of the vm. In the case of @hoppscotch/js-sandbox, multiple references to external objects are passed into the vm context to allow pre-request scripts interactions with environment variables and more. But this also allows the pre-request script to escape the sandbox. This vulnerability is fixed in 0.8.0.   |
| Node.js | 20.17.0 | CVE-2023-42955 | ['MEDIUM', 'MEDIUM'] | [4.9, 6.1] | Clarifai International has successfully resolved an issue of potentially exposing password information to front-end websites when signed in to the Admin Console with an administrator role. This issue has been fixed in FileMaker Server 20.3.1 by eliminating the send of Admin Role passwords in the Node.js socket.  |
| Node.js | 20.17.0 | CVE-2024-34710 | HIGH                 | 7.1        | Wiki.js is a wiki app built on Node.js. Client side template injection was discovered, that could allow an attacker to inject malicious JavaScript into the content section of pages that would execute once a victim loads the page that contains the payload. This was possible through the injection of an invalid HTML tag with a template injection payload on the next line. This vulnerability is fixed in 2.5.303.  |
| Node.js | 20.17.0 | CVE-2024-35237 | HIGH                 | 7.5        | MIT IdentiBot is an open-source Discord bot written in Node.js that verifies individuals' affiliations with MIT, grants them roles in a Discord server, and stores information about them in a database backend. A vulnerability that exists prior to commit 48e3e5e7ead6777fa75d57c7711c8e55b501c24e impacts all users who have performed verification with an instance of MIT IdentiBot that meets the following conditions: The instance of IdentiBot is tied to a "public" Discord application, i.e., users other than the API access registrant can add it to servers; *and* the instance has not yet been patched. In affected versions, IdentiBot does not check that a server is authorized before allowing members to execute slash and user commands in that server. As a result, any user can join IdentiBot to their server and then use commands (e.g., `/kerbid`) to reveal the full name and other information about a Discord user who has verified their affiliation with MIT using IdentiBot. The latest version o... |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2024-29415 | HIGH                 | 8.1        | The ip package through 2.0.1 for Node.js might allow SSRF because some IP addresses (such as 127.1, 01200034567, 012.1.2.3, 000:0:0000::01, and ::FFFF:127.0.0.1) are improperly categorized as globally routable via isPublic. NOTE: this issue exists because of an incomplete fix for CVE-2023-42282.  |
| Node.js | 20.17.0 | CVE-2024-37890 | HIGH                 | 7.5        | ws is an open source WebSocket client and server for Node.js. A request with a number of headers exceeding the server.maxHeadersCount threshold could be used to crash a ws server. The vulnerability was fixed in ws@8.17.1 (e55e510) and backported to ws@7.5.10 (22c2876), ws@6.2.3 (eeb76d3), and ws@5.2.4 (4abd8f6). In vulnerable versions of ws, the issue can be mitigated in the following ways: 1. Reduce the maximum allowed length of the request headers using the --max-http-header-size=size and/or the maxHeaderSize options so that no more headers than the server.maxHeadersCount limit can be sent. 2. Set server.maxHeadersCount to 0 so that no limit is applied. |
| Node.js | 20.17.0 | CVE-2024-38355 | HIGH                 | 7.3        | Socket.IO is an open source, real-time, bidirectional, event-based, communication framework. A specially crafted Socket.IO packet can trigger an uncaught exception on the Socket.IO server, thus killing the Node.js process. This issue is fixed by commit `15af22fc22` which has been included in `socket.io@4.6.2` (released in May 2023). The fix was backported in the 2.x branch as well with commit `d30630ba10`. Users are advised to upgrade. Users unable to upgrade may attach a listener for the "error" event to catch these errors.  |
| Node.js | 20.17.0 | CVE-2024-39309 | CRITICAL             | 9.8        | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. A vulnerability in versions prior to 6.5.7 and 7.1.0 allows SQL injection when Parse Server is configured to use the PostgreSQL database. The algorithm to detect SQL injection has been improved in versions 6.5.7 and 7.1.0. No known workarounds are available.  |
| Node.js | 20.17.0 | CVE-2024-39943 | ['CRITICAL', 'HIGH'] | [9.9, 8.8] | rejetto HFS (aka HTTP File Server) 3 before 0.52.10 on Linux, UNIX, and macOS allows OS command execution by remote authenticated users (if they have Upload permissions). This occurs because a shell is used to execute df (i.e., with execSync instead of spawnSync in child_process in Node.js).  |

|         |         |                |        |      |  |
|---------|---------|----------------|--------|------|--|
| Node.js | 20.17.0 | CVE-2024-39691 | MEDIUM | 4.3  | matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. The fix for GHSA-wm4w-7h2q-3pf7 / CVE-2024-32000 included in matrix-appservice-irc 2.0.0 relied on the Matrix homeserver-provided timestamp to determine whether a user has access to the event they're replying to when determining whether or not to include a truncated version of the original event in the IRC message. Since this value is controlled by external entities, a malicious Matrix homeserver joined to a room in which a matrix-appservice-irc bridge instance (before version 2.0.1) is present can fabricate the timestamp with the intent of tricking the bridge into leaking room messages the homeserver should not have access to. matrix-appservice-irc 2.0.1 drops the reliance on `origin_server_ts` when determining whether or not an event should be visible to a user, instead tracking the event timestamps internally. As a workaround, it's possible to limit the amount of information leaked by setting a reply... |
| Node.js | 20.17.0 | CVE-2024-38372 | LOW    | 2.0  | Undici is an HTTP/1.1 client, written from scratch for Node.js. Depending on network and process conditions of a `fetch()` request, `response.arrayBuffer()` might include portion of memory from the Node.js process. This has been patched in v6.19.2.   |
| Node.js | 20.17.0 | CVE-2024-22020 | None   | None | A security flaw in Node.js allows a bypass of network import restrictions. By embedding non-network imports in data URLs, an attacker can execute arbitrary code, compromising system security. Verified on various platforms, the vulnerability is mitigated by forbidding data URLs in network imports. Exploiting this flaw can violate network import security, posing a risk to developers and servers.   |
| Node.js | 20.17.0 | CVE-2024-22018 | None   | None | A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-read flag is used. This flaw arises from an inadequate permission model that fails to restrict file stats through the fs.lstat API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 21. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.   |

|         |         |                |                        |            |  |
|---------|---------|----------------|------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2024-42459 | MEDIUM                 | 5.3        | In the Elliptic package 6.5.6 for Node.js, EDDSA signature malleability occurs because there is a missing signature length check, and thus zero-valued bytes can be removed or appended.   |
| Node.js | 20.17.0 | CVE-2024-42460 | MEDIUM                 | 5.3        | In the Elliptic package 6.5.6 for Node.js, ECDSA signature malleability occurs because there is a missing check for whether the leading bit of r and s is zero.  |
| Node.js | 20.17.0 | CVE-2024-42461 | ['CRITICAL', 'MEDIUM'] | [9.1, 5.3] | In the Elliptic package 6.5.6 for Node.js, ECDSA signature malleability occurs because BER-encoded signatures are allowed.   |
| Node.js | 20.17.0 | CVE-2024-22169 | None                   | None       | WD Discovery versions prior to 5.0.589 contain a misconfiguration in the Node.js environment settings that could allow code execution by utilizing the 'ELECTRON_RUN_AS_NODE' environment variable. Any malicious application operating with standard user permissions can exploit this vulnerability, enabling code execution within WD Discovery application's context. WD Discovery version 5.0.589 addresses this issue by disabling certain features and fuses in Electron. The attack vector for this issue requires the victim to have the WD Discovery app installed on their device.  |
| Node.js | 20.17.0 | CVE-2024-43373 | ['HIGH', 'HIGH']       | [7.7, 7.8] | webcrack is a tool for reverse engineering javascript. An arbitrary file write vulnerability exists in the webcrack module when processing specifically crafted malicious code on Windows systems. This vulnerability is triggered when using the unpack bundles feature in conjunction with the saving feature. If a module name includes a path traversal sequence with Windows path separators, an attacker can exploit this to overwrite files on the host system. This vulnerability allows an attacker to write arbitrary '.js' files to the host system, which can be leveraged to hijack legitimate Node.js modules to gain arbitrary code execution. This vulnerability has been patched in version 2.14.1. |
| Node.js | 20.17.0 | CVE-2024-43409 | ['MEDIUM', 'MEDIUM']   | [6.5, 6.5] | Ghost is a Node.js content management system. Improper authentication on some endpoints used for member actions would allow an attacker to perform member-only actions, and read member information. This security vulnerability is present in Ghost v4.46.0-v5.89.4. v5.89.5 contains a fix for this issue.   |

|         |         |                |        |     |   |
|---------|---------|----------------|--------|-----|---|
| Node.js | 20.17.0 | CVE-2023-30582 | MEDIUM | 5.3 | A vulnerability has been identified in Node.js version 20, affecting users of the experimental permission model when the <code>--allow-fs-read</code> flag is used with a non- <code>*</code> argument. This flaw arises from an inadequate permission model that fails to restrict file watching through the <code>fs.watchFile</code> API. As a result, malicious actors can monitor files that they do not have explicit read access to. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.   |
| Node.js | 20.17.0 | CVE-2023-30583 | HIGH   | 7.5 | <code>fs.openAsBlob()</code> can bypass the experimental permission model when using the file system read restriction with the <code>--allow-fs-read</code> flag in Node.js 20. This flaw arises from a missing check in the <code>fs.openAsBlob()</code> API. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2023-30584 | HIGH   | 7.7 | A vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model. This flaw relates to improper handling of path traversal bypass when verifying file permissions. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.  |
| Node.js | 20.17.0 | CVE-2023-30587 | HIGH   | 7.5 | A vulnerability in Node.js version 20 allows for bypassing restrictions set by the <code>--experimental-permission</code> flag using the built-in inspector module ( <code>node:inspector</code> ). By exploiting the Worker class's ability to create an "internal worker" with the <code>klsInternal</code> Symbol, attackers can modify the <code>isInternal</code> value when an inspector is attached within the Worker constructor before initializing a new <code>WorkerImpl</code> . This vulnerability exclusively affects Node.js users employing the permission model mechanism. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. |
| Node.js | 20.17.0 | CVE-2023-39333 | MEDIUM | 5.3 | Maliciously crafted export names in an imported WebAssembly module can inject JavaScript code. The injected code may be able to access data and functions that the WebAssembly module itself does not have access to, similar to as if the WebAssembly module was a JavaScript module. This vulnerability affects users of any active release line of Node.js. The vulnerable feature is only available if Node.js is started with the <code>--experimental-wasm-modules</code> command line option.  |

|         |         |                |                  |            |   |
|---------|---------|----------------|------------------|------------|---|
| Node.js | 20.17.0 | CVE-2023-46809 | HIGH             | 7.4        | Node.js versions which bundle an unpatched version of OpenSSL or run against a dynamically linked version of OpenSSL which are unpatched are vulnerable to the Marvin Attack - <a href="https://people.redhat.com/~hkario/marvin/">https://people.redhat.com/~hkario/marvin/</a> , if PKCS #1 v1.5 padding is allowed when performing RSA decryption using a private key.   |
| Node.js | 20.17.0 | CVE-2024-36137 | None             | None       | A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-write flag is used. Node.js Permission Model do not operate on file descriptors, however, operations such as fs.fchown or fs.fchmod can use a "read-only" file descriptor to change the owner and permissions of a file.   |
| Node.js | 20.17.0 | CVE-2024-45590 | ['HIGH', 'HIGH'] | [7.5, 7.5] | body-parser is Node.js body parsing middleware. body-parser <1.20.3 is vulnerable to denial of service when url encoding is enabled. A malicious actor using a specially crafted payload could flood the server with a large number of requests, resulting in denial of service. This issue is patched in 1.20.3.   |
| Node.js | 20.17.0 | CVE-2024-45298 | MEDIUM           | 4.3        | Wiki.js is an open source wiki app built on Node.js. A disabled user can still gain access to a wiki by abusing the password reset function. While setting up SMTP e-mail's on my server, I tested said e-mails by performing a password reset with my test user. To my shock, not only did it let me reset my password, but after resetting my password I can get into the wiki I was locked out of. The ramifications of this bug is a user can <b>bypass an account disabling by requesting their password be reset</b> . All users of wiki.js version `2.5.303` who use any account restrictions and have disabled user are affected. This issue has been addressed in version 2.5.304 and all users are advised to upgrade. There are no known workarounds for this vulnerability. |
| Node.js | 20.17.0 | CVE-2024-47183 | ['HIGH', 'HIGH'] | [8.1, 8.1] | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. If the Parse Server option allowCustomObjectId: true is set, an attacker that is allowed to create a new user can set a custom object ID for that new user that exploits the vulnerability and acquires privileges of a specific role. This vulnerability is fixed in 6.5.9 and 7.3.0.  |

|         |         |                |                          |            |  |
|---------|---------|----------------|--------------------------|------------|--|
| Node.js | 20.17.0 | CVE-2024-45277 | ['MEDIUM', 'MEDIUM']     | [4.3, 4.3] | The SAP HANA Node.js client package versions from 2.0.0 before 2.21.31 is impacted by Prototype Pollution vulnerability allowing an attacker to add arbitrary properties to global object prototypes. This is due to improper user input sanitation when using the nestTables feature causing low impact on the availability of the application. This has no impact on Confidentiality and Integrity.                      |
| Node.js | 20.17.0 | CVE-2024-21532 | HIGH                     | 7.3        | All versions of the package ggjt are vulnerable to Command Injection via the fetchTags(branch) API, which allows user input to specify the branch to be fetched and then concatenates this string along with a git command which is then passed to the unsafe exec() Node.js child process API.  |
| Node.js | 20.17.0 | CVE-2024-48949 | ['CRITICAL', 'CRITICAL'] | [9.1, 9.1] | The verify function in lib/elliptic/eddsa/index.js in the Elliptic package before 6.5.6 for Node.js omits "sig.S().gte(sig.eddsa.curve.n)    sig.S().isNeg()" validation.  |
| Node.js | 20.17.0 | CVE-2024-48948 | MEDIUM                   | 4.8        | The Elliptic package 6.5.7 for Node.js, in its for ECDSA implementation, does not correctly verify valid signatures if the hash contains at least four leading 0 bytes and when the order of the elliptic curve's base point is smaller than the hash, because of an _truncateToN anomaly. This leads to valid signatures being rejected. Legitimate transactions or communications may be incorrectly flagged as invalid. |
| Node.js | 20.17.0 | CVE-2024-21536 | ['HIGH', 'HIGH']         | [7.5, 7.5] | Versions of the package http-proxy-middleware before 2.0.7, from 3.0.0 and before 3.0.3 are vulnerable to Denial of Service (DoS) due to an UnhandledPromiseRejection error thrown by micromatch. An attacker could kill the Node.js process and crash the server by making requests to certain paths.   |

|         |         |                |                      |            |   |
|---------|---------|----------------|----------------------|------------|---|
| Node.js | 20.17.0 | CVE-2024-48930 | None                 | None       | secp256k1-node is a Node.js binding for an Optimized C library for EC operations on curve secp256k1. In `elliptic`-based version, `loadUncompressedPublicKey` has a check that the public key is on the curve. Prior to versions 5.0.1, 4.0.4, and 3.8.1, however, `loadCompressedPublicKey` is missing that check. That allows the attacker to use public keys on low-cardinality curves to extract enough information to fully restore the private key from as little as 11 ECDH sessions, and very cheaply on compute power. Other operations on public keys are also affected, including e.g. `publicKeyVerify()` incorrectly returning `true` on those invalid keys, and e.g. `publicKeyTweakMul()` also returning predictable outcomes allowing to restore the tweak. Versions 5.0.1, 4.0.4, and 3.8.1 contain a fix for the issue. |
| Node.js | 20.17.0 | CVE-2020-26311 | HIGH                 | 7.5        | Useragent is a user agent parser for Node.js. All versions as of time of publication contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no patches are available.  |
| Node.js | 20.17.0 | CVE-2024-49770 | None                 | None       | `oak` is a middleware framework for Deno's native HTTP server, Deno Deploy, Node.js 16.5 and later, Cloudflare Workers and Bun. By default `oak` does not allow transferring of hidden files with `Context.send` API. However, prior to version 17.1.3, this can be bypassed by encoding `/` as its URL encoded form `%2F`. For an attacker this has potential to read sensitive user data or to gain access to server secrets. Version 17.1.3 fixes the issue.   |
| Node.js | 20.17.0 | CVE-2024-52505 | MEDIUM               | 5.4        | matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. The provisioning API of the matrix-appservice-irc bridge up to version 3.0.2 contains a vulnerability which can lead to arbitrary IRC command execution as the bridge IRC bot. The vulnerability has been patched in matrix-appservice-irc version 3.0.3.  |
| Node.js | 20.17.0 | CVE-2024-49362 | ['HIGH', 'CRITICAL'] | [7.7, 9.6] | Joplin is a free, open source note taking and to-do application. Joplin-desktop has a vulnerability that leads to remote code execution (RCE) when a user clicks on an <a> link within untrusted notes. The issue arises due to insufficient sanitization of <a> tag attributes introduced by the Mermaid. This vulnerability allows the execution of untrusted HTML content within the Electron window, which has full access to Node.js APIs, enabling arbitrary shell command execution.   |

|         |         |                |          |      |   |
|---------|---------|----------------|----------|------|---|
| Node.js | 20.17.0 | CVE-2024-53843 | HIGH     | 8.1  | <p>@dapperduckling/keycloak-connector-server is an opinionated series of libraries for Node.js applications and frontend clients to interface with keycloak. A Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the authentication flow of the application. This issue arises due to improper sanitization of the URL parameters, allowing the URL bar's contents to be injected and reflected into the HTML page. An attacker could craft a malicious URL to execute arbitrary JavaScript in the browser of a victim who visits the link. Any application utilizing this authentication library is vulnerable. Users of the application are at risk if they can be lured into clicking on a crafted malicious link. The vulnerability has been patched in version 2.5.5 by ensuring proper sanitization and escaping of user input in the affected URL parameters. Users are strongly encouraged to upgrade. If upgrading is not immediately possible, users can implement the following workarounds: 1. Employ a W...</p> |
| Node.js | 20.17.0 | CVE-2024-52810 | None     | None | <p>@intlify/shared is a shared library for the intlify project. The latest version of @intlify/shared (10.0.4) is vulnerable to Prototype Pollution through the entry function(s) lib.deepCopy. An attacker can supply a payload with Object.prototype.setter to introduce or modify properties within the global prototype chain, causing denial of service (DoS) as the minimum consequence. Moreover, the consequences of this vulnerability can escalate to other injection-based attacks, depending on how the library integrates within the application. For instance, if the polluted property propagates to sensitive Node.js APIs (e.g., exec, eval), it could enable an attacker to execute arbitrary commands within the application's context. This issue has been addressed in versions 9.14.2, and 10.0.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.</p>   |
| Node.js | 20.17.0 | CVE-2024-12641 | CRITICAL | 9.6  | <p>TenderDocTransfer from Chunghwa Telecom has a Reflected Cross-site scripting vulnerability. The application sets up a simple local web server and provides APIs for communication with the target website. Due to the lack of CSRF protection for the APIs, unauthenticated remote attackers could use specific APIs through phishing to execute arbitrary JavaScript code in the user's browser. Since the web server set by the application supports Node.js features, attackers can further leverage this to run OS commands.</p>   |

|         |         |                |      |      |   |
|---------|---------|----------------|------|------|---|
| Node.js | 20.17.0 | CVE-2024-56334 | HIGH | 7.8  | systeminformation is a System and OS information library for node.js. In affected versions SSIDs are not sanitized when before they are passed as a parameter to cmd.exe in the <code>`getWindowsIEEE8021x`</code> function. This means that malicious content in the SSID can be executed as OS commands. This vulnerability may enable an attacker, depending on how the package is used, to perform remote code execution or local privilege escalation. This issue has been addressed in version 5.23.7 and all users are advised to upgrade. There are no known workarounds for this vulnerability.  |
| Node.js | 20.17.0 | CVE-2024-52006 | None | None | Git is a fast, scalable, distributed revision control system with an unusually rich command set that provides both high-level operations and full access to internals. Git defines a line-based protocol that is used to exchange information between Git and Git credential helpers. Some ecosystems (most notably, .NET and node.js) interpret single Carriage Return characters as newlines, which renders the protections against CVE-2020-5260 incomplete for credential helpers that treat Carriage Returns in this way. This issue has been addressed in commit <code>`b01b9b8`</code> which is included in release versions v2.48.1, v2.47.2, v2.46.3, v2.45.3, v2.44.3, v2.43.6, v2.42.4, v2.41.3, and v2.40.4. Users are advised to upgrade. Users unable to upgrade should avoid cloning from untrusted URLs, especially recursive clones. |
| Node.js | 20.17.0 | CVE-2025-23083 | None | None | With the aid of the <code>diagnostics_channel</code> utility, an event can be hooked into whenever a worker thread is created. This is not limited only to workers but also exposes internal workers, where an instance of them can be fetched, and its constructor can be grabbed and reinstated for malicious usage. This vulnerability affects Permission Model users ( <code>--permission</code> ) on Node.js v20, v22, and v23.  |
| Node.js | 20.17.0 | CVE-2025-23090 | None | None | With the aid of the <code>diagnostics_channel</code> utility, an event can be hooked into whenever a worker thread is created. This is not limited only to workers but also exposes internal workers, where an instance of them can be fetched, and its constructor can be grabbed and reinstated for malicious usage. This vulnerability affects Permission Model users ( <code>--permission</code> ) on Node.js v20, v22, and v23.  |

|         |         |                |      |      |   |
|---------|---------|----------------|------|------|---|
| Node.js | 20.17.0 | CVE-2025-23084 | None | None | A vulnerability has been identified in Node.js, specifically affecting the handling of drive names in the Windows environment. Certain Node.js functions do not treat drive names as special on Windows. As a result, although Node.js assumes a relative path, it actually refers to the root directory. On Windows, a path that does not start with the file separator is treated as relative to the current directory. This vulnerability affects Windows users of `path.join` API.  |
| Node.js | 20.17.0 | CVE-2025-23085 | None | None | A memory leak could occur when a remote peer abruptly closes the socket without sending a GOAWAY notification. Additionally, if an invalid header was detected by nghttp2, causing the connection to be terminated by the peer, the same leak was triggered. This flaw could lead to increased memory consumption and potential denial of service under certain conditions. This vulnerability affects HTTP/2 Server users on Node.js v18.x, v20.x, v22.x and v23.x.  |
| Node.js | 20.17.0 | CVE-2025-24876 | HIGH | 8.1  | The SAP Approuter Node.js package version v16.7.1 and before is vulnerable to Authentication bypass. When trading an authorization code an attacker can steal the session of the victim by injecting malicious payload causing High impact on confidentiality and integrity of the application  |
| Node.js | 20.17.0 | CVE-2025-25200 | None | None | Koa is expressive middleware for Node.js using ES2017 async functions. Prior to versions 0.21.2, 1.7.1, 2.15.4, and 3.0.0-alpha.3, Koa uses an evil regex to parse the `X-Forwarded-Proto` and `X-Forwarded-Host` HTTP headers. This can be exploited to carry out a Denial-of-Service attack. Versions 0.21.2, 1.7.1, 2.15.4, and 3.0.0-alpha.3 fix the issue.   |
| Node.js | 20.17.0 | CVE-2025-25283 | HIGH | 7.5  | parse-duration is software that allows users to convert a human readable duration to milliseconds. Versions prior to 2.1.3 are vulnerable to an event loop delay due to the CPU-bound operation of resolving the provided string, from a 0.5ms and up to ~50ms per one operation, with a varying size from 0.01 MB and up to 4.3 MB respectively, and an out of memory that would crash a running Node.js application due to a string size of roughly 10 MB that utilizes unicode characters. Version 2.1.3 contains a patch. |

|         |         |                |                   |            |  |
|---------|---------|----------------|-------------------|------------|--|
| Node.js | 20.17.0 | CVE-2025-27146 | ['LOW', 'MEDIUM'] | [2.7, 4.3] | matrix-appservice-irc is a Node.js IRC bridge for Matrix. The matrix-appservice-irc bridge up to version 3.0.3 contains a vulnerability which can lead to arbitrary IRC command execution as the puppeted user. The attacker can only inject commands executed as their own IRC user. The vulnerability has been patched in matrix-appservice-irc version 3.0.4.   |
| Node.js | 20.17.0 | CVE-2025-27152 | None              | None       | axios is a promise based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if <code>baseURL</code> is set, axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of axios. This issue is fixed in 1.8.2.  |
| Node.js | 20.17.0 | CVE-2025-27597 | None              | None       | Vue I18n is the internationalization plugin for Vue.js. <code>@intlify/message-resolver</code> and <code>@intlify/vue-i18n-core</code> are vulnerable to Prototype Pollution through the entry function: <code>handleFlatJson</code> . An attacker can supply a payload with <code>Object.prototype.setter</code> to introduce or modify properties within the global prototype chain, causing denial of service (DoS) as the minimum consequence. Moreover, the consequences of this vulnerability can escalate to other injection-based attacks, depending on how the library integrates within the application. For instance, if the polluted property propagates to sensitive Node.js APIs (e.g., <code>exec</code> , <code>eval</code> ), it could enable an attacker to execute arbitrary commands within the application's context. |
| Node.js | 20.17.0 | CVE-2024-28607 | LOW               | 2.9        | The ip-utils package through 2.4.0 for Node.js might allow SSRF because some IP addresses (such as <code>0x7f.1</code> ) are improperly categorized as globally routable via a falsy <code>isPrivate</code> return value.  |

|         |         |                |      |      |   |
|---------|---------|----------------|------|------|---|
| Node.js | 20.17.0 | CVE-2025-29774 | None | None | xml-crypto is an XML digital signature and encryption library for Node.js. An attacker may be able to exploit a vulnerability in versions prior to 6.0.1, 3.2.1, and 2.1.6 to bypass authentication or authorization mechanisms in systems that rely on xml-crypto for verifying signed XML documents. The vulnerability allows an attacker to modify a valid signed XML message in a way that still passes signature verification checks. For example, it could be used to alter critical identity or access control attributes, enabling an attacker with a valid account to escalate privileges or impersonate another user. Users of versions 6.0.0 and prior should upgrade to version 6.0.1 to receive a fix. Those who are still using v2.x or v3.x should upgrade to patched versions 2.1.6 or 3.2.1, respectively. |
| Node.js | 20.17.0 | CVE-2025-29775 | None | None | xml-crypto is an XML digital signature and encryption library for Node.js. An attacker may be able to exploit a vulnerability in versions prior to 6.0.1, 3.2.1, and 2.1.6 to bypass authentication or authorization mechanisms in systems that rely on xml-crypto for verifying signed XML documents. The vulnerability allows an attacker to modify a valid signed XML message in a way that still passes signature verification checks. For example, it could be used to alter critical identity or access control attributes, enabling an attacker to escalate privileges or impersonate another user. Users of versions 6.0.0 and prior should upgrade to version 6.0.1 to receive a fix. Those who are still using v2.x or v3.x should upgrade to patched versions 2.1.6 or 3.2.1, respectively.                      |

|         |         |                |        |     |  |
|---------|---------|----------------|--------|-----|--|
| Node.js | 20.17.0 | CVE-2025-30168 | MEDIUM | 6.9 | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 7.5.2 and 8.0.2, the 3rd party authentication handling of Parse Server allows the authentication credentials of some specific authentication providers to be used across multiple Parse Server apps. For example, if a user signed up using the same authentication provider in two unrelated Parse Server apps, the credentials stored by one app can be used to authenticate the same user in the other app. Note that this only affects Parse Server apps that specifically use an affected 3rd party authentication provider for user authentication, for example by setting the Parse Server option auth to configure a Parse Server authentication adapter. The fix of this vulnerability requires to upgrade Parse Server to a version that includes the bug fix, as well as upgrade the client app to send a secure payload, which is different from the previous insecure payload. This vulnerability is fi... |
| Node.js | 20.17.0 | CVE-2025-32379 | MEDIUM | 5.0 | Koa is expressive middleware for Node.js using ES2017 async functions. In koa < 2.16.1 and < 3.0.0-alpha.5, passing untrusted user input to ctx.redirect() even after sanitizing it, may execute javascript code on the user who use the app. This issue is patched in 2.16.1 and 3.0.0-alpha.5.   |
| Node.js | 20.17.0 | CVE-2025-32442 | HIGH   | 7.5 | Fastify is a fast and low overhead web framework, for Node.js. In versions 5.0.0 to 5.3.0 as well as version 4.9.0, applications that specify different validation strategies for different content types have a possibility to bypass validation by providing a _slightly altered_ content type such as with different casing or altered whitespace before `;`. This was patched in v5.3.1, but the initial patch did not cover all problems. This has been fully patched in v5.3.2 and v4.9.1. A workaround involves not specifying individual content types in the schema.  |

|         |         |                |        |      |   |
|---------|---------|----------------|--------|------|---|
| Node.js | 20.17.0 | CVE-2025-32965 | None   | None | <p>xrpl.js is a JavaScript/TypeScript API for interacting with the XRP Ledger in Node.js and the browser. Versions 4.2.1, 4.2.2, 4.2.3, and 4.2.4 of xrpl.js were compromised and contained malicious code designed to exfiltrate private keys. Version 2.14.2 is also malicious, though it is less likely to lead to exploitation as it is not compatible with other 2.x versions. Anyone who used one of these versions should stop immediately and rotate any private keys or secrets used with affected systems. Users of xrpl.js should upgrade to version 4.2.5 or 2.14.3 to receive a patch. To secure funds, think carefully about whether any keys may have been compromised by this supply chain attack, and mitigate by sending funds to secure wallets, and/or rotating keys. If any account's master key is potentially compromised, disable the key.</p>  |
| Node.js | 20.17.0 | CVE-2025-47153 | MEDIUM | 6.5  | <p>Certain build processes for libuv and Node.js for 32-bit systems, such as for the nodejs binary package through nodejs_20.19.0+dfsg-2_i386.deb for Debian GNU/Linux, have an inconsistent off_t size (e.g., building on i386 Debian always uses _FILE_OFFSET_BITS=64 for the libuv dynamic library, but uses the _FILE_OFFSET_BITS global system default of 32 for nodejs), leading to out-of-bounds access. NOTE: this is not a problem in the Node.js software itself. In particular, the Node.js website's download page does not offer prebuilt Node.js for Linux on i386.</p>   |
| Node.js | 20.17.0 | CVE-2025-46720 | LOW    | 3.1  | <p>Keystone is a content management system for Node.js. Prior to version 6.5.0, <code>{field}.isFilterable`</code> access control can be bypassed in <code>`update`</code> and <code>`delete`</code> mutations by adding additional unique filters. These filters can be used as an oracle to probe the existence or value of otherwise unreadable fields. Specifically, when a mutation includes a <code>`where`</code> clause with multiple unique filters (e.g. <code>`id`</code> and <code>`email`</code>), Keystone will attempt to match records even if filtering by the latter fields would normally be rejected by <code>`field.isFilterable`</code> or <code>`list.defaultIsFilterable`</code>. This can allow malicious actors to infer the presence of a particular field value when a filter is successful in returning a result. This affects any project relying on the default or dynamic <code>`isFilterable`</code> behavior (at the list or field level) to prevent external users from using the filtering of fields as a discovery mechanism. While this access control is respected during <code>`findMany`</code> operations, it was not complete...</p> |

|                             |          |                |      |      |   |
|-----------------------------|----------|----------------|------|------|---|
| Npcap                       | 1.79     | CVE-2019-11490 | None | None | An issue was discovered in Npcap 0.992. Sending a malformed .pcap file with the loopback adapter using either pcap_sendqueue_queue() or pcap_sendqueue_transmit() results in kernel pool corruption. This could lead to arbitrary code executing inside the Windows kernel and allow escalation of privileges.  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2017-8622  | None | None | Windows Subsystem for Linux in Windows 10 1703 allows an elevation of privilege vulnerability when it fails to properly handle handles NT pipes, aka "Windows Subsystem for Linux Elevation of Privilege Vulnerability".  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2017-8627  | None | None | Windows Subsystem for Linux in Windows 10 1703, allows a denial of service vulnerability due to the way it handles objects in memory, aka "Windows Subsystem for Linux Denial of Service Vulnerability".  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2017-8703  | None | None | The Microsoft Windows Subsystem for Linux on Microsoft Windows 10 1703 allows a denial of service vulnerability when it improperly handles objects in memory, aka "Windows Subsystem for Linux Denial of Service Vulnerability".  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2018-0743  | None | None | Windows Subsystem for Linux in Windows 10 version 1703, Windows 10 version 1709, and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka "Windows Subsystem for Linux Elevation of Privilege Vulnerability".  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2018-0334  | None | None | A vulnerability in the certificate management subsystem of Cisco AnyConnect Network Access Manager and of Cisco AnyConnect Secure Mobility Client for iOS, Mac OS X, Android, Windows, and Linux could allow an unauthenticated, remote attacker to bypass the TLS certificate check when downloading certain configuration files. The vulnerability is due to improper use of Simple Certificate Enrollment Protocol and improper server certificate validation. An attacker could exploit this vulnerability by preparing malicious profile and localization files for Cisco AnyConnect to use. A successful exploit could allow the attacker to remotely change the configuration profile, a certificate, or the localization data used by AnyConnect Secure Mobility Client. Cisco Bug IDs: CSCvh23141. |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2018-8337  | None | None | A security feature bypass vulnerability exists when Windows Subsystem for Linux improperly handles case sensitivity, aka "Windows Subsystem for Linux Security Feature Bypass Vulnerability." This affects Windows 10, Windows 10 Servers.  |

|                             |          |               |      |      |  |
|-----------------------------|----------|---------------|------|------|--|
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2018-8441 | None | None | An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka "Windows Subsystem for Linux Elevation of Privilege Vulnerability." This affects Windows 10, Windows 10 Servers.   |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2018-8329 | None | None | An Elevation of Privilege vulnerability exists in Windows Subsystem for Linux when it fails to properly handle objects in memory, aka "Linux On Windows Elevation Of Privilege Vulnerability." This affects Windows 10, Windows 10 Servers.                              |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0553 | None | None | An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka "Windows Subsystem for Linux Information Disclosure Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019.          |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0682 | None | None | An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0689, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0689 | None | None | An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0692 | None | None | An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0693, CVE-2019-0694. |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0693 | None | None | An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0694. |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0694 | None | None | An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0693. |

|                             |          |               |          |     |   |
|-----------------------------|----------|---------------|----------|-----|---|
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-1185 | HIGH     | 7.3 | An elevation of privilege vulnerability exists due to a stack corruption in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory.  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-1416 | HIGH     | 7.0 | An elevation of privilege vulnerability exists due to a race condition in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'.  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-0155 | HIGH     | 7.8 | Insufficient access control in a subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6, E-2100 and E-2200 Processor Families; Intel(R) Graphics Driver for Windows before 26.20.100.6813 (DCH) or 26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077), i915 Linux Driver for Intel(R) Processor Graphics before versions 5.4-rc7, 5.3.11, 4.19.84, 4.14.154, 4.9.201, 4.4.201 may allow an authenticated user to potentially enable escalation of privilege via local access. |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2020-0636 | HIGH     | 7.8 | An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'.   |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2019-1353 | CRITICAL | 9.8 | An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. When running Git in the Windows Subsystem for Linux (also known as "WSL") while accessing a working directory on a regular Windows drive, none of the NTFS protections were active.   |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2020-1075 | MEDIUM   | 5.5 | An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka 'Windows Subsystem for Linux Information Disclosure Vulnerability'.   |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2020-1423 | HIGH     | 7.8 | An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'.   |

|                             |          |                |                  |            |   |
|-----------------------------|----------|----------------|------------------|------------|---|
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2021-36966 | ['HIGH', 'HIGH'] | [7.8, 7.8] | Windows Subsystem for Linux Elevation of Privilege Vulnerability  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2022-38014 | HIGH             | 7.0        | Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2022-44689 | ['HIGH', 'HIGH'] | [7.8, 7.8] | Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2024-20681 | HIGH             | 7.8        | Windows Subsystem for Linux Elevation of Privilege Vulnerability  |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2025-24084 | HIGH             | 8.4        | Untrusted pointer dereference in Windows Subsystem for Linux allows an unauthorized attacker to execute code locally.   |
| Windows Subsystem for Linux | 2.4.13.0 | CVE-2025-26675 | HIGH             | 7.8        | Out-of-bounds read in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.  |
| XAMPP                       | 8.2.12-0 | CVE-2005-1077  | None             | None       | Multiple cross-site scripting (XSS) vulnerabilities in XAMPP 1.4.x allow remote attackers to inject arbitrary web script or HTML via (1) cds.php, (2) Guestbook-EN.pl, or (3) phonebook.php.  |
| XAMPP                       | 8.2.12-0 | CVE-2005-1078  | None             | None       | XAMPP 1.4.x has multiple default or null passwords, which allows attackers to gain privileges.  |
| XAMPP                       | 8.2.12-0 | CVE-2005-2043  | None             | None       | Directory traversal vulnerability in XAMPP before 1.4.14 allows remote attackers to inject arbitrary HTML and PHP code via lang.php.  |
| XAMPP                       | 8.2.12-0 | CVE-2006-4994  | None             | None       | Multiple unquoted Windows search path vulnerabilities in Apache Friends XAMPP 1.5.2 might allow local users to gain privileges via a malicious program file in %SYSTEMDRIVE%, which is run when XAMPP attempts to execute (1) FileZillaServer.exe, (2) mysqld-nt.exe, (3) Perl.exe, or (4) xamppcontrol.exe with an unquoted "Program Files" pathname.  |
| XAMPP                       | 8.2.12-0 | CVE-2007-2079  | None             | None       | The ADONewConnection Connect function in adodb.php in XAMPP 1.6.0a and earlier for Windows uses untrusted input for the database server hostname, which allows remote attackers to trigger a library buffer overflow and execute arbitrary code via a long host parameter, or have other unspecified impact. NOTE: it could be argued that this is an issue in mssql_connect (CVE-2007-1411.1) in PHP, or an issue in the ADOdb Library, and the proper fix should be in one of these products; if so, then this should not be treated as a vulnerability in XAMPP. |
| XAMPP                       | 8.2.12-0 | CVE-2007-2080  | None             | None       | Multiple SQL injection vulnerabilities in XAMPP 1.6.0a for Windows allow remote attackers to execute arbitrary SQL commands via unspecified vectors in certain test scripts.  |

|       |          |               |      |      |   |
|-------|----------|---------------|------|------|---|
| XAMPP | 8.2.12-0 | CVE-2008-3569 | None | None | Multiple cross-site scripting (XSS) vulnerabilities in XAMPP 1.6.7, when register_globals is enabled, allow remote attackers to inject arbitrary web script or HTML via the text parameter to (1) iart.php and (2) ming.php.  |
| XAMPP | 8.2.12-0 | CVE-2008-4450 | None | None | Cross-site scripting (XSS) vulnerability in adodb.php in XAMPP for Windows 1.6.8 allows remote attackers to inject arbitrary web script or HTML via the (1) dbserver, (2) host, (3) user, (4) password, (5) database, and (6) table parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.  |
| XAMPP | 8.2.12-0 | CVE-2009-0919 | None | None | XAMPP installs multiple packages with insecure default passwords, which makes it easier for remote attackers to obtain access via (1) the "lamp" default password for the "nobody" account within the included ProFTPD installation, (2) a blank default password for the "root" account within the included MySQL installation, (3) a blank default password for the "pma" account within the phpMyAdmin installation, and possibly other unspecified passwords. NOTE: this was originally reported as a problem in DFLabs PTK, but this issue affects any product that is installed within the XAMPP environment, and should not be viewed as a vulnerability within that product. NOTE: DFLabs states that PTK is intended for use in a laboratory with "no contact from / to internet." |
| XAMPP | 8.2.12-0 | CVE-2008-6498 | None | None | Cross-site request forgery (CSRF) vulnerability in security/xamppsecurity.php in XAMPP 1.6.8 allows remote attackers to hijack the authentication of users for requests that change a certain .htaccess password via the xampppasswd parameter.   |
| XAMPP | 8.2.12-0 | CVE-2008-6499 | None | None | security/xamppsecurity.php in XAMPP 1.6.8 performs an extract operation on the SERVER superglobal array, which allows remote attackers to spoof critical variables, as demonstrated by setting the REMOTE_ADDR variable to 127.0.0.1.   |
| XAMPP | 8.2.12-0 | CVE-2013-2586 | None | None | XAMPP 1.8.1 does not properly restrict access to xampp/lang.php, which allows remote attackers to modify xampp/lang.tmp and execute cross-site scripting (XSS) attacks via the WriteIntoLocalDisk method.   |

|       |          |                |                      |            |  |
|-------|----------|----------------|----------------------|------------|--|
| XAMPP | 8.2.12-0 | CVE-2018-17933 | None                 | None       | VGo Robot (Versions 3.0.3.52164 and 3.0.3.53662. Prior versions may also be affected) connected to the VGo XAMPP. User accounts may be able to execute commands that are outside the scope of their privileges and within the scope of an admin account. If an attacker has access to VGo XAMPP Client credentials, they may be able to execute admin commands on the connected robot. |
| XAMPP | 8.2.12-0 | CVE-2019-8923  | None                 | None       | XAMPP through 5.6.8 and previous allows SQL injection via the cds-fpdf.php Jahr parameter. NOTE: This product is discontinued.   |
| XAMPP | 8.2.12-0 | CVE-2019-8924  | None                 | None       | XAMPP through 5.6.8 allows XSS via the cds-fpdf.php interpret or titel parameter. NOTE: This product is discontinued.  |
| XAMPP | 8.2.12-0 | CVE-2019-8920  | None                 | None       | lart.php in XAMPP 1.7.0 has XSS, a related issue to CVE-2008-3569.   |
| XAMPP | 8.2.12-0 | CVE-2020-11107 | HIGH                 | 8.8        | An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16, and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-control.ini for all users (including admins) to enable arbitrary command execution.  |
| XAMPP | 8.2.12-0 | CVE-2022-29376 | HIGH                 | 8.8        | Xampp for Windows v8.1.4 and below was discovered to contain insecure permissions for its install directory, allowing attackers to execute arbitrary code via overwriting binaries located in the directory.   |
| XAMPP | 8.2.12-0 | CVE-2017-20018 | ['MEDIUM', 'HIGH']   | [6.3, 7.8] | A vulnerability was found in XAMPP 7.1.1-0-VC14. It has been classified as problematic. Affected is an unknown function of the component Installer. The manipulation leads to privilege escalation. It is possible to launch the attack remotely.  |
| XAMPP | 8.2.12-0 | CVE-2022-47637 | MEDIUM               | 6.7        | The installer in XAMPP through 8.1.12 allows local users to write to the C:\xampp directory. Common use cases execute files under C:\xampp with administrative privileges.   |
| XAMPP | 8.2.12-0 | CVE-2024-0338  | ['HIGH', 'CRITICAL'] | [7.3, 9.8] | A buffer overflow vulnerability has been found in XAMPP affecting version 8.2.4 and earlier. An attacker could execute arbitrary code through a long file debug argument that controls the Structured Exception Handler (SEH).   |
| XAMPP | 8.2.12-0 | CVE-2024-5055  | HIGH                 | 7.5        | Uncontrolled resource consumption vulnerability in XAMPP Windows, versions 7.3.2 and earlier. This vulnerability exists when XAMPP attempts to process many incomplete HTTP requests, resulting in resource consumption and system crashes.  |