# National Critical Information Infrastructure Protection Centre

## Common Vulnerabilities and Exposures(CVE) Report

**01 - 15 Mar 2020 Vol. 07 No. 05**

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Alfresco** | | | | | |
| **alfresco** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-03-2020 | 3.5 | Alfresco Enterprise before 5.2.7 and Alfresco Community before 6.2.0 (rb65251d6-b368) has XSS via the URL property of a file. **CVE ID : CVE-2020-8776** | N/A | A-ALF-ALFR-160320/1 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-03-2020 | 3.5 | Alfresco Enterprise before 5.2.7 and Alfresco Community before 6.2.0 (rb65251d6-b368) has XSS via a user profile photo, as demonstrated by a SCRIPT element in an SVG document. **CVE ID : CVE-2020-8777** | N/A | A-ALF-ALFR-160320/2 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-03-2020 | 3.5 | Alfresco Enterprise before 5.2.7 and Alfresco Community before 6.2.0 (rb65251d6-b368) has XSS via an uploaded document, when the attacker has write access to a project. **CVE ID : CVE-2020-8778** | N/A | A-ALF-ALFR-160320/3 |
| **Apache** | | | | | |
| **shardingsphere** | | | | | |
| Deserialization of | 11-03-2020 | 7.5 | In Apache ShardingSphere(incubator | https://lists.apache.org/t | A-APA-SHAR- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Data | | | ) 4.0.0-RC3 and 4.0.0, the ShardingSphere's web console uses the SnakeYAML library for parsing YAML inputs to load datasource configuration. SnakeYAML allows to unmarshal data to a Java type By using the YAML tag. Unmarshalling untrusted data can lead to security flaws of RCE.<br>**CVE ID : CVE-2020-1947** | hread.html/r4a61a24c119bd820da6fb02100d286f8aae55c8f9b94a346b9bb27d8%40%3Cdev.shardingsphere.apache.org%3E | 160320/4 |
| **Artica** | | | | | |
| **pandora_fms** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 02-03-2020 | 6.5 | ** DISPUTED ** In Artica Pandora FMS 7.42, Web Admin users can execute arbitrary code by uploading a .php file via the Updater or Extension component. NOTE: The vendor reports that this is intended functionality.<br>**CVE ID : CVE-2020-8500** | N/A | A-ART-PAND-160320/5 |
| **Avast** | | | | | |
| **antitrack** | | | | | |
| Improper Certificate Validation | 09-03-2020 | 5.8 | Avast AntiTrack before 1.5.1.172 and AVG Antitrack before 2.0.0.178 proxies traffic to HTTPS sites but does not validate certificates, and thus a man-in-the-middle can host a malicious website using a self-signed certificate. No special action necessary by the victim using AntiTrack | https://www.avast.com/hacker-hall-of-fame/en/researcher-david-eade-reports-antitrack-bug-to-avast | A-AVA-ANTI-160320/6 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | with "Allow filtering of HTTPS traffic for tracking detection" enabled. (This is the default configuration.)<br>**CVE ID : CVE-2020-8987** | | |
| **avg_antitrack** | | | | | |
| Improper Certificate Validation | 09-03-2020 | 5.8 | Avast AntiTrack before 1.5.1.172 and AVG Antitrack before 2.0.0.178 proxies traffic to HTTPS sites but does not validate certificates, and thus a man-in-the-middle can host a malicious website using a self-signed certificate. No special action necessary by the victim using AntiTrack with "Allow filtering of HTTPS traffic for tracking detection" enabled. (This is the default configuration.)<br>**CVE ID : CVE-2020-8987** | https://www.avast.com/hacker-hall-of-fame/en/researcher-david-eade-reports-antitrack-bug-to-avast | A-AVA-AVG_-160320/7 |
| **Bittorrent** | | | | | |
| **utorrent** | | | | | |
| Improper Input Validation | 02-03-2020 | 5 | The bencoding parser in BitTorrent uTorrent through 3.5.5 (build 45505) misparses nested bencoded dictionaries, which allows a remote attacker to cause a denial of service.<br>**CVE ID : CVE-2020-8437** | https://utclient.utorrent.com/offers/beta_release_notes/release_notes.html | A-BIT-UTOR-160320/8 |
| **bookstackapp** | | | | | |
| **bookstack** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unrestricted Upload of File with Dangerous Type | 09-03-2020 | 9 | BookStack before version 0.25.5 has a vulnerability where a user could upload PHP files through image upload functions, which would allow them to execute code on the host system remotely. They would then have the permissions of the PHP process. This most impacts scenarios where non-trusted users are given permission to upload images in any area of the application. The issue was addressed in a series of patches in versions 0.25.3, 0.25.4 and 0.25.5. Users should upgrade to at least v0.25.5 to avoid this vulnerability. **CVE ID : CVE-2020-5256** | https://github.com/BookStackApp/BookStack/security/advisories/GHSA-g9rq-x4fj-f5hx | A-BOO-BOOK-160320/9 |
| **chadhaajay** | | | | | |
| **phpkb** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-subscribers.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10430** | N/A | A-CHA-PHPK-160320/10 |
| Improper Neutralization of Input | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard | N/A | A-CHA-PHPK-160320/11 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-templates.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10431** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-tickets.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10432** | N/A | A-CHA-PHPK-160320/12 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-users.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10433** | N/A | A-CHA-PHPK-160320/13 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-versions.php by adding a question mark (?) followed | N/A | A-CHA-PHPK-160320/14 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by the payload.<br>**CVE ID : CVE-2020-10434** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/my-languages.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10435** | N/A | A-CHA-PHPK-160320/15 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/my-profile.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10436** | N/A | A-CHA-PHPK-160320/16 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/optimize-database.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10437** | N/A | A-CHA-PHPK-160320/17 |
| Improper Neutralization of Input During Web | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows | N/A | A-CHA-PHPK-160320/18 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Page Generation ('Cross-site Scripting') | | | Reflected XSS (injecting arbitrary web script or HTML) in admin/reply-ticket.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10438** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-discussed.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10439** | N/A | A-CHA-PHPK-160320/19 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-mailed.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10440** | N/A | A-CHA-PHPK-160320/20 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-monthly.php by adding a question mark (?) followed by the payload. | N/A | A-CHA-PHPK-160320/21 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10441** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-popular.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10442** | N/A | A-CHA-PHPK-160320/22 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-printed.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10443** | N/A | A-CHA-PHPK-160320/23 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 12-03-2020 | 4 | Path Traversal in admin/download.php in Chadha PHPKB Standard Multi-Language 9 allows remote attackers to download files from the server using a dot-dot-slash sequence (../) via the GET parameter file.<br>**CVE ID : CVE-2020-10387** | N/A | A-CHA-PHPK-160320/24 |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 4.3 | The way the Referer header in article.php is handled in Chadha PHPKB Standard Multi-Language 9 allows attackers to execute Stored (Blind) XSS | N/A | A-CHA-PHPK-160320/25 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | (injecting arbitrary web script or HTML) in admin/report-referrers.php (vulnerable file admin/include/functions-articles.php).<br>**CVE ID : CVE-2020-10388** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 12-03-2020 | 6.5 | OS Command Injection in export.php (vulnerable function called from include/functions-article.php) in Chadha PHPKB Standard Multi-Language 9 allows remote attackers to achieve Code Execution by saving the code to be executed as the wkhtmltopdf path via admin/save-settings.php.<br>**CVE ID : CVE-2020-10390** | N/A | A-CHA-PHPK-160320/26 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-article.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10391** | N/A | A-CHA-PHPK-160320/27 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add- | N/A | A-CHA-PHPK-160320/28 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | category.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10392** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-field.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10393** | N/A | A-CHA-PHPK-160320/29 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-glossary.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10394** | N/A | A-CHA-PHPK-160320/30 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-group.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10395** | N/A | A-CHA-PHPK-160320/31 |
| Improper Neutralizatio | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in | N/A | A-CHA-PHPK- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-language.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10396** | | 160320/32 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-news.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10397** | N/A | A-CHA-PHPK-160320/33 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-template.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10398** | N/A | A-CHA-PHPK-160320/34 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-user.php by adding a | N/A | A-CHA-PHPK-160320/35 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10399** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/article-collaboration.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10400** | N/A | A-CHA-PHPK-160320/36 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-article.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10401** | N/A | A-CHA-PHPK-160320/37 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-category.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10402** | N/A | A-CHA-PHPK-160320/38 |
| Improper Neutralization of Input | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard | N/A | A-CHA-PHPK- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-comment.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10403** | | 160320/39 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-field.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10404** | N/A | A-CHA-PHPK-160320/40 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-glossary.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10405** | N/A | A-CHA-PHPK-160320/41 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-group.php by adding a question mark (?) followed | N/A | A-CHA-PHPK-160320/42 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by the payload.<br>**CVE ID : CVE-2020-10406** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-news.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10407** | N/A | A-CHA-PHPK-160320/43 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-subscriber.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10408** | N/A | A-CHA-PHPK-160320/44 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-template.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10409** | N/A | A-CHA-PHPK-160320/45 |
| Improper Neutralization of Input During Web | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows | N/A | A-CHA-PHPK-160320/46 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Page Generation ('Cross-site Scripting') | | | Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-user.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10410** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/email-harvester.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10411** | N/A | A-CHA-PHPK-160320/47 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/import-csv.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10412** | N/A | A-CHA-PHPK-160320/48 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/import-html.php by adding a question mark (?) followed by the payload. | N/A | A-CHA-PHPK-160320/49 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10413** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/index-attachments.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10414** | N/A | A-CHA-PHPK-160320/50 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/index.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10415** | N/A | A-CHA-PHPK-160320/51 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/kb-backup.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10416** | N/A | A-CHA-PHPK-160320/52 |
| Improper Neutralization of Input During Web Page | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting | N/A | A-CHA-PHPK-160320/53 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | arbitrary web script or HTML) in admin/manage-articles.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10417** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-attachments.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10418** | N/A | A-CHA-PHPK-160320/54 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-categories.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10419** | N/A | A-CHA-PHPK-160320/55 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-comments.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10420** | N/A | A-CHA-PHPK-160320/56 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-departments.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10421** | N/A | A-CHA-PHPK-160320/57 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-drafts.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10422** | N/A | A-CHA-PHPK-160320/58 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-feedbacks.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10423** | N/A | A-CHA-PHPK-160320/59 |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or | N/A | A-CHA-PHPK-160320/60 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | HTML) in admin/manage-fields.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10424** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-glossary.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10425** | N/A | A-CHA-PHPK-160320/61 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-groups.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10426** | N/A | A-CHA-PHPK-160320/62 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-languages.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10427** | N/A | A-CHA-PHPK-160320/63 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-news.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10428** | N/A | A-CHA-PHPK-160320/64 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-settings.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10429** | N/A | A-CHA-PHPK-160320/65 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-rated.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10444** | N/A | A-CHA-PHPK-160320/66 |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or | N/A | A-CHA-PHPK-160320/67 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | HTML) in admin/report-article.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10445** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-category.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10446** | N/A | A-CHA-PHPK-160320/68 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-failed-login.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10447** | N/A | A-CHA-PHPK-160320/69 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-search.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10449** | N/A | A-CHA-PHPK-160320/70 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-traffic.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10450** | N/A | A-CHA-PHPK-160320/71 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-user.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10451** | N/A | A-CHA-PHPK-160320/72 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/save-article.php by adding a question mark (?) followed by the payload. **CVE ID : CVE-2020-10452** | N/A | A-CHA-PHPK-160320/73 |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or | N/A | A-CHA-PHPK-160320/74 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | HTML) in admin/search-users.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10453** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/sitemap-generator.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10454** | N/A | A-CHA-PHPK-160320/75 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/translate.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10455** | N/A | A-CHA-PHPK-160320/76 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/trash-box.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10456** | N/A | A-CHA-PHPK-160320/77 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 12-03-2020 | 4 | Path Traversal in admin/imagepaster/image-renaming.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to rename any file on the webserver using a dot-dot-slash sequence (../) via the POST parameter imgName (for the new name) and imgUrl (for the current file to be renamed).<br>**CVE ID : CVE-2020-10457** | N/A | A-CHA-PHPK-160320/78 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 12-03-2020 | 5.5 | Path Traversal in admin/imagepaster/operations.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete any folder on the webserver using a dot-dot-slash sequence (../) via the GET parameter crdir, when the GET parameter action is set to df, causing a Denial of Service.<br>**CVE ID : CVE-2020-10458** | N/A | A-CHA-PHPK-160320/79 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 12-03-2020 | 4 | Path Traversal in admin/assetmanager/assetmanager.php (vulnerable function saved in admin/assetmanager/functions.php) in Chadha PHPKB Standard Multi-Language 9 allows attackers to list the files that are stored on the webserver using a dot-dot-slash sequence (../) via the | N/A | A-CHA-PHPK-160320/80 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | POST parameter inpCurrFolder.<br>**CVE ID : CVE-2020-10459** | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 12-03-2020 | 4 | admin/include/operations.php (via admin/email-harvester.php) in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject untrusted input inside CSV files via the POST parameter data.<br>**CVE ID : CVE-2020-10460** | N/A | A-CHA-PHPK-160320/81 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 4.3 | The way comments in article.php (vulnerable function in include/functions-article.php) are handled in Chadha PHPKB Standard Multi-Language 9 allows attackers to execute Stored (Blind) XSS (injecting arbitrary web script or HTML) in admin/manage-comments.php, via the GET parameter cmt.<br>**CVE ID : CVE-2020-10461** | N/A | A-CHA-PHPK-160320/82 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-field.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10462** | N/A | A-CHA-PHPK-160320/83 |
| Improper Neutralization of Input | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-template.php in Chadha PHPKB | N/A | A-CHA-PHPK- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10463** | | 160320/84 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-article.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10464** | N/A | A-CHA-PHPK-160320/85 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-category.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10465** | N/A | A-CHA-PHPK-160320/86 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10466** | N/A | A-CHA-PHPK-160320/87 |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-comment.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or | N/A | A-CHA-PHPK-160320/88 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10467** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/edit-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.<br>**CVE ID : CVE-2020-10468** | N/A | A-CHA-PHPK-160320/89 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10469** | N/A | A-CHA-PHPK-160320/90 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-fields.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10470** | N/A | A-CHA-PHPK-160320/91 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-articles.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET | N/A | A-CHA-PHPK-160320/92 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | parameter sort.<br>**CVE ID : CVE-2020-10471** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-templates.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10472** | N/A | A-CHA-PHPK-160320/93 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-categories.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10473** | N/A | A-CHA-PHPK-160320/94 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10474** | N/A | A-CHA-PHPK-160320/95 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-settings.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to change the global settings, potentially gaining code execution or | N/A | A-CHA-PHPK-160320/96 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | causing a denial of service, via a crafted request.<br>**CVE ID : CVE-2020-10478** | | |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/add-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new news article via a crafted request.<br>**CVE ID : CVE-2020-10479** | N/A | A-CHA-PHPK-160320/97 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/add-category.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new category via a crafted request.<br>**CVE ID : CVE-2020-10480** | N/A | A-CHA-PHPK-160320/98 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/add-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new glossary term via a crafted request.<br>**CVE ID : CVE-2020-10481** | N/A | A-CHA-PHPK-160320/99 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/add-template.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new article template via a crafted request.<br>**CVE ID : CVE-2020-10482** | N/A | A-CHA-PHPK-160320/100 |
| Cross-Site Request Forgery | 12-03-2020 | 4.3 | CSRF in admin/ajax-hub.php in Chadha PHPKB Standard Multi-Language 9 | N/A | A-CHA-PHPK-160320/101 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| (CSRF) | | | allows attackers to post a comment on any article via a crafted request.<br>**CVE ID : CVE-2020-10483** | | |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/add-field.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to create a custom field via a crafted request.<br>**CVE ID : CVE-2020-10484** | N/A | A-CHA-PHPK-160320/102 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-articles.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete an article via a crafted request.<br>**CVE ID : CVE-2020-10485** | N/A | A-CHA-PHPK-160320/103 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a comment via a crafted request.<br>**CVE ID : CVE-2020-10486** | N/A | A-CHA-PHPK-160320/104 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a glossary term via a crafted request.<br>**CVE ID : CVE-2020-10487** | N/A | A-CHA-PHPK-160320/105 |
| Cross-Site Request Forgery | 12-03-2020 | 4.3 | CSRF in admin/manage-news.php in Chadha PHPKB Standard Multi- | N/A | A-CHA-PHPK-160320/106 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| (CSRF) | | | Language 9 allows attackers to delete a news article via a crafted request.<br>**CVE ID : CVE-2020-10488** | | |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-tickets.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a ticket via a crafted request.<br>**CVE ID : CVE-2020-10489** | N/A | A-CHA-PHPK-160320/107 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a department via a crafted request.<br>**CVE ID : CVE-2020-10490** | N/A | A-CHA-PHPK-160320/108 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a department via a crafted request.<br>**CVE ID : CVE-2020-10491** | N/A | A-CHA-PHPK-160320/109 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-templates.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete an article template via a crafted request.<br>**CVE ID : CVE-2020-10492** | N/A | A-CHA-PHPK-160320/110 |
| Cross-Site Request | 12-03-2020 | 4.3 | CSRF in admin/edit-glossary.php in Chadha | N/A | A-CHA-PHPK- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Forgery (CSRF) | | | PHPKB Standard Multi-Language 9 allows attackers to edit a glossary term, given the id, via a crafted request.<br>**CVE ID : CVE-2020-10493** | | 160320/111 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/edit-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a news article, given the id, via a crafted request.<br>**CVE ID : CVE-2020-10494** | N/A | A-CHA-PHPK-160320/112 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/edit-template.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit an article template, given the id, via a crafted request.<br>**CVE ID : CVE-2020-10495** | N/A | A-CHA-PHPK-160320/113 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/edit-article.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit an article, given the id, via a crafted request.<br>**CVE ID : CVE-2020-10496** | N/A | A-CHA-PHPK-160320/114 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-categories.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a category via a crafted request.<br>**CVE ID : CVE-2020-10497** | N/A | A-CHA-PHPK-160320/115 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/edit-category.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a category, given the id, via a crafted request. **CVE ID : CVE-2020-10498** | N/A | A-CHA-PHPK-160320/116 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-tickets.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to close any ticket, given the id, via a crafted request. **CVE ID : CVE-2020-10499** | N/A | A-CHA-PHPK-160320/117 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/reply-ticket.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to reply to any ticket, given the id, via a crafted request. **CVE ID : CVE-2020-10500** | N/A | A-CHA-PHPK-160320/118 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a department, given the id, via a crafted request. **CVE ID : CVE-2020-10501** | N/A | A-CHA-PHPK-160320/119 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to approve any comment, given the id, via | N/A | A-CHA-PHPK-160320/120 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | a crafted request.<br>**CVE ID : CVE-2020-10502** | | |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to disapprove any comment, given the id, via a crafted request.<br>**CVE ID : CVE-2020-10503** | N/A | A-CHA-PHPK-160320/121 |
| Cross-Site Request Forgery (CSRF) | 12-03-2020 | 4.3 | CSRF in admin/edit-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a comment, given the id, via a crafted request.<br>**CVE ID : CVE-2020-10504** | N/A | A-CHA-PHPK-160320/122 |
| **Cisco** | | | | | |
| **content_security_management_appliance** | | | | | |
| Improper Input Validation | 04-03-2020 | 5 | A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Content Security Management Appliance (SMA) could allow an unauthenticated remote attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper validation of specific HTTP request headers. An attacker could | N/A | A-CIS-CONT-160320/123 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to trigger a prolonged status of high CPU utilization relative to the GUI process(es). Upon successful exploitation of this vulnerability, an affected device will still be operative, but its response time and overall performance may be degraded.<br>**CVE ID : CVE-2020-3164** | | |
| **jabber** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration | N/A | A-CIS-JABB-160320/124 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **email_security_appliance** | | | | | |
| Improper Input Validation | 04-03-2020 | 5 | A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Content Security Management Appliance (SMA) could allow an unauthenticated remote attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to | N/A | A-CIS-EMAI-160320/125 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | improper validation of specific HTTP request headers. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to trigger a prolonged status of high CPU utilization relative to the GUI process(es). Upon successful exploitation of this vulnerability, an affected device will still be operative, but its response time and overall performance may be degraded.<br>**CVE ID : CVE-2020-3164** | | |
| Uncontrolled Resource Consumption | 04-03-2020 | 6.4 | A vulnerability in the malware detection functionality in Cisco Advanced Malware Protection (AMP) in Cisco AsyncOS Software for Cisco Email Security Appliances (ESAs) could allow an unauthenticated remote attacker to exhaust resources on an affected device. The vulnerability is due to insufficient control over system memory allocation. An attacker could exploit this vulnerability by sending a crafted email through the targeted device. A successful exploit could | N/A | A-CIS-EMAI-160320/126 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allow the attacker to cause an email attachment that contains malware to be delivered to a user and cause email processing delays.<br>**CVE ID : CVE-2020-3181** | | |
| **prime_network_registrar** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-03-2020 | 4.3 | A vulnerability in the web-based interface of Cisco Prime Network Registrar (CPNR) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections in the web-based interface. An attacker could exploit this vulnerability by persuading a targeted user, with an active administrative session on the affected device, to click a malicious link. A successful exploit could allow an attacker to change the device's configuration, which could include the ability to edit or create user accounts of any privilege level. Some changes to the device's configuration could negatively impact the availability of networking services for other devices | N/A | A-CIS-PRIM-160320/127 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on networks managed by CPNR.<br>**CVE ID : CVE-2020-3148** | | |
| **webex_teams** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content | N/A | A-CIS-WEBE-160320/128 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **webex_meetings_online** | | | | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted | N/A | A-CIS-WEBE-160320/129 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | user.<br>**CVE ID : CVE-2020-3127** | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3128** | N/A | A-CIS-WEBE-160320/130 |
| **webex_meetings_server** | | | | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and | N/A | A-CIS-WEBE-160320/131 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3127** | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a | N/A | A-CIS-WEBE-160320/132 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3128** | | |
| **webex_network_recording_player** | | | | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could | N/A | A-CIS-WEBE-160320/133 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3127** | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful | N/A | A-CIS-WEBE-160320/134 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3128** | | |
| **intelligence_proximity** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the | N/A | A-CIS-INTE-160320/135 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **meeting** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the | N/A | A-CIS-MEET-160320/136 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **prime_collaboration_provisioning** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-03-2020 | 4.3 | A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script | N/A | A-CIS-PRIM-160320/137 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | code in the context of the interface or access sensitive, browser-based information.<br>**CVE ID : CVE-2020-3192** | | |
| Information Exposure | 04-03-2020 | 5 | A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to obtain sensitive information about an affected device. The vulnerability exists because replies from the web-based management interface include unnecessary server information. An attacker could exploit this vulnerability by inspecting replies received from the web-based management interface. A successful exploit could allow the attacker to obtain details about the operating system, including the web server version that is running on the device, which could be used to perform further attacks.<br>**CVE ID : CVE-2020-3193** | N/A | A-CIS-PRIM-160320/138 |
| **telepresence_management_suite** | | | | | |
| Improper Neutralization of Input During Web Page | 04-03-2020 | 3.5 | A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow an | N/A | A-CIS-TELE-160320/139 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web-based management interface or access sensitive, browser-based information.<br>**CVE ID : CVE-2020-3185** | | |
| **web_security_appliance** | | | | | |
| Improper Input Validation | 04-03-2020 | 5 | A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Content Security Management Appliance (SMA) could allow an unauthenticated remote attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to | N/A | A-CIS-WEB_-160320/140 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | improper validation of specific HTTP request headers. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to trigger a prolonged status of high CPU utilization relative to the GUI process(es). Upon successful exploitation of this vulnerability, an affected device will still be operative, but its response time and overall performance may be degraded.<br>**CVE ID : CVE-2020-3164** | | |
| **identity_services_engine** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-03-2020 | 3.5 | A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by crafting a malicious configuration | N/A | A-CIS-IDEN-160320/141 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and saving it to the targeted system. An exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information when an administrator views the configuration. An attacker would need write permissions to exploit this vulnerability successfully.<br>**CVE ID : CVE-2020-3157** | | |
| **webex_meetings** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man | N/A | A-CIS-WEBE-160320/142 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| Information Exposure | 04-03-2020 | 3.3 | A vulnerability in the multicast DNS (mDNS) protocol configuration of Cisco Webex Meetings Client for MacOS could allow an unauthenticated adjacent attacker to obtain sensitive information about the device on which the Webex client is running. The vulnerability exists because sensitive information is included in the mDNS reply. An attacker could exploit this vulnerability by doing an mDNS query for a particular service against an affected device. A successful exploit could allow the attacker to gain | N/A | A-CIS-WEBE-160320/143 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | access to sensitive information.<br>**CVE ID : CVE-2020-3182** | | |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3127** | N/A | A-CIS-WEBE-160320/144 |
| Improper Input Validation | 04-03-2020 | 9.3 | Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and | N/A | A-CIS-WEBE-160320/145 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.<br>**CVE ID : CVE-2020-3128** | | |
| **cloud_email_security** | | | | | |
| Improper Input Validation | 04-03-2020 | 5 | A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Content Security Management Appliance (SMA) could allow an unauthenticated | N/A | A-CIS-CLOU-160320/146 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | remote attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper validation of specific HTTP request headers. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to trigger a prolonged status of high CPU utilization relative to the GUI process(es). Upon successful exploitation of this vulnerability, an affected device will still be operative, but its response time and overall performance may be degraded.<br>**CVE ID : CVE-2020-3164** | | |
| **Ckeditor** | | | | | |
| **ckeditor** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 4.3 | A cross-site scripting (XSS) vulnerability in the WSC plugin through 5.5.7.5 for CKEditor 4 allows remote attackers to run arbitrary web script inside an IFRAME element by injecting a crafted HTML element into the editor.<br>**CVE ID : CVE-2020-9440** | N/A | A-CKE-CKED-160320/147 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 07-03-2020 | 4.3 | A cross-site scripting (XSS) vulnerability in the HTML Data Processor for CKEditor 4.0 before 4.14 allows remote attackers to inject arbitrary web script through a crafted "protected" comment (with the cke_protected syntax).<br>**CVE ID : CVE-2020-9281** | N/A | A-CKE-CKED-160320/148 |
| **cncf** | | | | | |
| **envoy** | | | | | |
| Uncontrolled Resource Consumption | 04-03-2020 | 5 | CNCF Envoy through 1.13.0 may consume excessive amounts of memory when proxying HTTP/1.1 requests or responses with many small (i.e. 1 byte) chunks.<br>**CVE ID : CVE-2020-8659** | https://www.envoyproxy.io/docs/envoy/v1.13.1/intro/version_history | A-CNC-ENVO-160320/149 |
| Uncontrolled Resource Consumption | 04-03-2020 | 5 | CNCF Envoy through 1.13.0 may consume excessive amounts of memory when responding internally to pipelined requests.<br>**CVE ID : CVE-2020-8661** | https://www.envoyproxy.io/docs/envoy/v1.13.1/intro/version_history | A-CNC-ENVO-160320/150 |
| Incorrect Authorization | 04-03-2020 | 7.5 | CNCF Envoy through 1.13.0 has incorrect Access Control when using SDS with Combined Validation Context. Using the same secret (e.g. trusted CA) across many resources together with the combined validation context could lead to the "static" part of the | https://www.envoyproxy.io/docs/envoy/v1.13.1/intro/version_history | A-CNC-ENVO-160320/151 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | validation context to be not applied, even though it was visible in the active config dump.<br>**CVE ID : CVE-2020-8664** | | |
| **Codepeople** | | | | | |
| **appointment_booking_calendar** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-03-2020 | 3.5 | Stored XSS exists in the Appointment Booking Calendar plugin before 1.3.35 for WordPress. In the cpabc_appointments.php file, the Calendar Name input could allow attackers to inject arbitrary JavaScript or HTML.<br>**CVE ID : CVE-2020-9371** | N/A | A-COD-APPO-160320/152 |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 04-03-2020 | 6.8 | The Appointment Booking Calendar plugin before 1.3.35 for WordPress allows user input (in fields such as Description or Name) in any booking form to be any formula, which then could be exported via the Bookings list tab in /wp-admin/admin.php?page=cpabc_appointments.php. The attacker could achieve remote code execution via CSV injection.<br>**CVE ID : CVE-2020-9372** | N/A | A-COD-APPO-160320/153 |
| **Craftcms** | | | | | |
| **craft_cms** | | | | | |
| Improper Neutralizatio | 04-03-2020 | 5 | The Seomatic component before 3.2.46 for Craft CMS | N/A | A-CRA-CRAF- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements in Output Used by a Downstream Component ('Injection') | | | allows Server-Side Template Injection and information disclosure via malformed data to the metacontainers controller.<br>**CVE ID : CVE-2020-9757** | | 160320/154 |
| **Creative-solutions** | | | | | |
| **creative_contact_form** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 04-03-2020 | 5 | An issue was discovered in helpers/mailer.php in the Creative Contact Form extension 4.6.2 before 2019-12-03 for Joomla!. A directory traversal vulnerability resides in the filename field for uploaded attachments via the creativecontactform_upload parameter. An attacker could exploit this vulnerability with the "Send me a copy" option to receive any files of the filesystem via email.<br>**CVE ID : CVE-2020-9364** | N/A | A-CRE-CREA-160320/155 |
| **Dell** | | | | | |
| **digital_delivery** | | | | | |
| Incorrect Default Permissions | 09-03-2020 | 7.2 | Dell Digital Delivery versions prior to 3.5.2015 contain an incorrect default permissions vulnerability. A locally authenticated low-privileged malicious user could exploit this vulnerability to run an arbitrary executable with administrative privileges | N/A | A-DEL-DIGI-160320/156 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on the affected system.<br>**CVE ID : CVE-2020-5342** | | |
| **emc_isilon_onefs** | | | | | |
| Missing Authenticati on for Critical Function | 06-03-2020 | 10 | Dell EMC Isilon OneFS versions prior to 8.2.0 contain an unauthorized access vulnerability due to a lack of thorough authorization checks when SyncIQ is licensed, but encrypted syncs are not marked as required. When this happens, loss of control of the cluster can occur.<br>**CVE ID : CVE-2020-5328** | N/A | A-DEL-EMC_-160320/157 |
| **security_management_server** | | | | | |
| Deserializati on of Untrusted Data | 06-03-2020 | 9.3 | Dell Security Management Server versions prior to 10.2.10 contain a Java RMI Deserialization of Untrusted Data vulnerability. When the server is exposed to the internet and Windows Firewall is disabled, a remote unauthenticated attacker may exploit this vulnerability by sending a crafted RMI request to execute arbitrary code on the target host.<br>**CVE ID : CVE-2020-5327** | N/A | A-DEL-SECU-160320/158 |
| **Djangoproject** | | | | | |
| **django** | | | | | |
| Improper Neutralizatio n of Special | 05-03-2020 | 7.5 | Django 1.11 before 1.11.29, 2.2 before 2.2.11, and 3.0 before 3.0.4 allows | https://ww w.djangoproj ect.com/web | A-DJA-DJAN-160320/159 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an SQL Command ('SQL Injection') | | | SQL Injection if untrusted data is used as a tolerance parameter in GIS functions and aggregates on Oracle. By passing a suitably crafted tolerance to GIS functions and aggregates on Oracle, it was possible to break escaping and inject malicious SQL.<br>**CVE ID : CVE-2020-9402** | log/2020/mar/04/security-releases/ | |
| **Emerson** | | | | | |
| **valvelink** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | In Emerson ValveLink v12.0.264 to v13.4.118, a vulnerability in the ValveLink software may allow a local, unprivileged, trusted insider to escalate privileges due to insecure configuration parameters.<br>**CVE ID : CVE-2020-6971** | N/A | A-EME-VALV-160320/160 |
| **envoyproxy** | | | | | |
| **envoy** | | | | | |
| Insufficient Verification of Data Authenticity | 04-03-2020 | 7.5 | CNCF Envoy through 1.13.0 TLS inspector bypass. TLS inspector could have been bypassed (not recognized as a TLS client) by a client using only TLS 1.3. Because TLS extensions (SNI, ALPN) were not inspected, those connections might have been matched to a wrong filter chain, possibly bypassing some security restrictions in the process. | https://www.envoyproxy.io/docs/envoy/v1.13.1/intro/version_history | A-ENV-ENVO-160320/161 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-8660** | | |
| **Eset** | | | | | |
| **cyber_security** | | | | | |
| Improper Input Validation | 05-03-2020 | 7.5 | The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10180** | N/A | A-ESE-CYBE-160320/162 |
| Improper Input Validation | 06-03-2020 | 5 | ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10193** | N/A | A-ESE-CYBE-160320/163 |
| **internet_security** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 06-03-2020 | 5 | ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10193** | N/A | A-ESE-INTE-160320/164 |
| **mobile_security** | | | | | |
| Improper Input Validation | 05-03-2020 | 7.5 | The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10180** | N/A | A-ESE-MOBI-160320/165 |
| Improper Input Validation | 06-03-2020 | 5 | ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information | N/A | A-ESE-MOBI-160320/166 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10193** | | |
| **nod32_antivirus** | | | | | |
| Improper Input Validation | 05-03-2020 | 7.5 | The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10180** | N/A | A-ESE-NOD3-160320/167 |
| Improper Input Validation | 06-03-2020 | 5 | ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security | N/A | A-ESE-NOD3-160320/168 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10193** | | |
| **smart_security** | | | | | |
| Improper Input Validation | 05-03-2020 | 7.5 | The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10180** | N/A | A-ESE-SMAR-160320/169 |
| Improper Input Validation | 06-03-2020 | 5 | ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for | N/A | A-ESE-SMAR-160320/170 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Linux Desktop.<br>**CVE ID : CVE-2020-10193** | | |
| **smart_tv_security** | | | | | |
| Improper Input Validation | 05-03-2020 | 7.5 | The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10180** | N/A | A-ESE-SMAR-160320/171 |
| Improper Input Validation | 06-03-2020 | 5 | ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.<br>**CVE ID : CVE-2020-10193** | N/A | A-ESE-SMAR-160320/172 |
| **Facebook** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **hhvm** | | | | | |
| Out-of-bounds Read | 03-03-2020 | 5 | Insufficient boundary checks when decoding JSON in handleBackslash reads out of bounds memory, potentially leading to DOS. This issue affects HHVM 4.45.0, 4.44.0, 4.43.0, 4.42.0, 4.41.0, 4.40.0, 4.39.0, versions between 4.33.0 and 4.38.0 (inclusive), versions between 4.9.0 and 4.32.0 (inclusive), and versions prior to 4.8.7. **CVE ID : CVE-2020-1888** | https://github.com/facebook/hhvm/commit/b3679121bb3c7017ff04b4c08402ffff5cf59b13, https://hhvm.com/blog/2020/02/20/security-update.html | A-FAC-HHVM-160320/173 |
| Out-of-bounds Read | 03-03-2020 | 6.4 | Insufficient boundary checks when decoding JSON in JSON_parser allows read access to out of bounds memory, potentially leading to information leak and DOS. This issue affects HHVM 4.45.0, 4.44.0, 4.43.0, 4.42.0, 4.41.0, 4.40.0, 4.39.0, versions between 4.33.0 and 4.38.0 (inclusive), versions between 4.9.0 and 4.32.0 (inclusive), and versions prior to 4.8.7. **CVE ID : CVE-2020-1892** | https://github.com/facebook/hhvm/commit/dabd48caf74995e605f1700344f1ff4a5d83441d, https://hhvm.com/blog/2020/02/20/security-update.html | A-FAC-HHVM-160320/174 |
| Out-of-bounds Read | 03-03-2020 | 5 | Insufficient boundary checks when decoding JSON in TryParse reads out of bounds memory, potentially leading to DOS. This issue affects HHVM 4.45.0, 4.44.0, 4.43.0, | https://github.com/facebook/hhvm/commit/bd586671a3c22eb2f07e55f11b3ce64e1f79 | A-FAC-HHVM-160320/175 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 4.42.0, 4.41.0, 4.40.0, 4.39.0, versions between 4.33.0 and 4.38.0 (inclusive), versions between 4.9.0 and 4.32.0 (inclusive), and versions prior to 4.8.7.<br>**CVE ID : CVE-2020-1893** | 61e7, https://hhvm.com/blog/2020/02/20/security-update.html | |
| **Fasterxml** | | | | | |
| **jackson-databind** | | | | | |
| Deserialization of Untrusted Data | 02-03-2020 | 6.8 | FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari.HikariConfig (aka shaded hikari-config).<br>**CVE ID : CVE-2020-9546** | N/A | A-FAS-JACK-160320/176 |
| Deserialization of Untrusted Data | 02-03-2020 | 6.8 | FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.ibatis.sqlmap.engine.transaction.jta.JtaTransactionConfig (aka ibatis-sqlmap).<br>**CVE ID : CVE-2020-9547** | N/A | A-FAS-JACK-160320/177 |
| Deserialization of Untrusted Data | 02-03-2020 | 6.8 | FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.Anter | N/A | A-FAS-JACK-160320/178 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | osDBCPConfig (aka anteros-core).<br>**CVE ID : CVE-2020-9548** | | |
| **fatfreeframework** | | | | | |
| **fat-free_framework** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 11-03-2020 | 7.5 | In Fat-Free Framework 3.7.1, attackers can achieve arbitrary code execution if developers choose to pass user controlled input (e.g., $_REQUEST, $_GET, or $_POST) to the framework's Clear method.<br>**CVE ID : CVE-2020-5203** | https://github.com/bcosca/fatfree-core/commit/dae95a0baf3963a9ef87c17cee52f78f77e21829 | A-FAT-FAT--160320/179 |
| **Froxlor** | | | | | |
| **froxlor** | | | | | |
| Improper Input Validation | 09-03-2020 | 6.5 | An issue was discovered in Froxlor before 0.10.14. Remote attackers with access to the installation routine could have executed arbitrary code via the database configuration options that were passed unescaped to exec, because of _backupExistingDatabase in install/lib/class.FroxlorInstall.php.<br>**CVE ID : CVE-2020-10235** | N/A | A-FRO-FROX-160320/180 |
| Improper Input Validation | 09-03-2020 | 3.6 | An issue was discovered in Froxlor before 0.10.14. It created files with static names in /tmp during installation if the | N/A | A-FRO-FROX-160320/181 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | installation directory was not writable. This allowed local attackers to cause DoS or disclose information out of the config files, because of _createUserdataConf in install/lib/class.FroxlorInstall.php.<br>**CVE ID : CVE-2020-10236** | | |
| Information Exposure | 09-03-2020 | 2.1 | An issue was discovered in Froxlor through 0.10.15. The installer wrote configuration parameters including passwords into files in /tmp, setting proper permissions only after writing the sensitive data. A local attacker could have disclosed the information if he read the file at the right time, because of _createUserdataConf in install/lib/class.FroxlorInstall.php.<br>**CVE ID : CVE-2020-10237** | N/A | A-FRO-FROX-160320/182 |
| **Gitlab** | | | | | |
| **gitlab** | | | | | |
| Improper Privilege Management | 06-03-2020 | 7.5 | GitLab 10.7 and later through 12.7.2 has Incorrect Access Control.<br>**CVE ID : CVE-2020-8113** | https://about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/ | A-GIT-GITL-160320/183 |
| **GNU** | | | | | |
| **glibc** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-03-2020 | 2.1 | The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d41414141414141000 0 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c. **CVE ID : CVE-2020-10029** | N/A | A-GNU-GLIB-160320/184 |
| **gonitro** | | | | | |
| **nitro_pro** | | | | | |
| Out-of-bounds Write | 08-03-2020 | 5.8 | npdf.dll in Nitro Pro before 13.13.2.242 is vulnerable to Heap Corruption at npdf!nitro::get_property+2381 via a crafted PDF document. **CVE ID : CVE-2020-10222** | N/A | A-GON-NITR-160320/185 |
| Out-of-bounds Write | 08-03-2020 | 5.8 | npdf.dll in Nitro Pro before 13.13.2.242 is vulnerable to JBIG2Decode CNxJBIG2DecodeStream Heap Corruption at npdf!CAPPDAnnotHandlerUtils::create_popup_for_markup+0x12fbe via a crafted PDF document. **CVE ID : CVE-2020-10223** | N/A | A-GON-NITR-160320/186 |
| **grandit** | | | | | |
| **grandit** | | | | | |
| Authorization Bypass | 02-03-2020 | 6.4 | GRANDIT Ver.1.6, Ver.2.0, Ver.2.1, Ver.2.2, Ver.2.3, | N/A | A-GRA-GRAN- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Through User-Controlled Key | | | and Ver.3.0 do not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and then alter or disclose the information via unspecified vectors.<br>**CVE ID : CVE-2020-5539** | | 160320/187 |
| **hcltech** | | | | | |
| **connections** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-03-2020 | 3.5 | The HCL Connections 5.5 help system is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.<br>**CVE ID : CVE-2020-4082** | https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0075447 | A-HCL-CONN-160320/188 |
| Information Exposure Through Log Files | 05-03-2020 | 2.1 | HCL Connections 6.5 is vulnerable to possible information leakage. Connections could disclose sensitive information via trace logs to a local user.<br>**CVE ID : CVE-2020-4083** | https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0075503 | A-HCL-CONN-160320/189 |
| Improper Neutralizatio | 09-03-2020 | 3.5 | HCL Connections v5.5, v6.0, and v6.5 are | https://support.hcltechs | A-HCL-CONN- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**CVE ID : CVE-2020-4084** | w.com/csm?id=kb_article&sysparm_article=KB0076649 | 160320/190 |
| **HP** | | | | | |
| **oneview_global_dashboard** | | | | | |
| Information Exposure | 04-03-2020 | 5 | HPE OneView Global Dashboard (OVGD) 1.9 has a remote information disclosure vulnerability. HPE OneView Global Dashboard - After Upgrade or Install of OVGD Version 1.9, Appliance Firewall May Leave Ports Open. This is resolved in OVGD 1.91 or later.<br>**CVE ID : CVE-2020-7130** | N/A | A-HP-ONEV-160320/191 |
| **IBM** | | | | | |
| **tivoli_netcool\/omnibus** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-03-2020 | 3.5 | IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | https://www.ibm.com/support/pages/node/5690828 | A-IBM-TIVO-160320/192 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IBM X-Force ID: 174907.<br>**CVE ID : CVE-2020-4196** | | |
| Insecure Storage of Sensitive Information | 03-03-2020 | 2.1 | IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 174908.<br>**CVE ID : CVE-2020-4197** | https://www.ibm.com/support/pages/node/5690822 | A-IBM-TIVO-160320/193 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-03-2020 | 3.5 | IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174909.<br>**CVE ID : CVE-2020-4198** | https://www.ibm.com/support/pages/node/5690840 | A-IBM-TIVO-160320/194 |
| **spectrum_scale** | | | | | |
| Improper Check for Unusual or Exceptional Conditions | 09-03-2020 | 5 | The IBM Spectrum Scale 4.2 and 5.0 file system component is affected by a denial of service security vulnerability. An attacker can force the Spectrum Scale mmfsd/mmsdrserv daemons to unexpectedly exit, impacting the functionality of the Spectrum Scale cluster and the availability of file systems managed by Spectrum Scale. IBM X- | https://www.ibm.com/support/pages/node/5693463 | A-IBM-SPEC-160320/195 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Force ID: 175067.<br>**CVE ID : CVE-2020-4217** | | |
| **security_information_queue** | | | | | |
| Use of Hard-coded Credentials | 02-03-2020 | 5 | IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, and 1.0.4 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 176206.<br>**CVE ID : CVE-2020-4283** | https://www.ibm.com/support/pages/node/5383395 | A-IBM-SECU-160320/196 |
| Information Exposure | 02-03-2020 | 5 | IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, and 1.0.4 uses a cross-domain policy file that includes domains that should not be trusted which could disclose sensitive information. IBM X-Force ID: 176335.<br>**CVE ID : CVE-2020-4292** | https://www.ibm.com/support/pages/node/5390193 | A-IBM-SECU-160320/197 |
| **platform_lsf** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | IBM Platform LSF 9.1 and 10.1, IBM Spectrum LSF Suite 10.2, and IBM Spectrum Suite for HPA 10.2 could allow a local user to escalate their privileges due to weak file permissions when specific debug settings are enabled in a Linux or Unix enviornment. IBM X-Force | https://www.ibm.com/support/pages/node/3357549 | A-IBM-PLAT-160320/198 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: 176137.<br>**CVE ID : CVE-2020-4278** | | |
| **spectrum_computing_for_high_performance_analytics** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | IBM Platform LSF 9.1 and 10.1, IBM Spectrum LSF Suite 10.2, and IBM Spectrum Suite for HPA 10.2 could allow a local user to escalate their privileges due to weak file permissions when specific debug settings are enabled in a Linux or Unix enviornment. IBM X-Force ID: 176137.<br>**CVE ID : CVE-2020-4278** | https://www.ibm.com/support/pages/node/3357549 | A-IBM-SPEC-160320/199 |
| **spectrum_lsf** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | IBM Platform LSF 9.1 and 10.1, IBM Spectrum LSF Suite 10.2, and IBM Spectrum Suite for HPA 10.2 could allow a local user to escalate their privileges due to weak file permissions when specific debug settings are enabled in a Linux or Unix enviornment. IBM X-Force ID: 176137.<br>**CVE ID : CVE-2020-4278** | https://www.ibm.com/support/pages/node/3357549 | A-IBM-SPEC-160320/200 |
| **infosphere_information_server** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 10-03-2020 | 3.5 | IBM InfoSphere Information Server 11.5 and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web | https://www.ibm.com/support/pages/node/5690451 | A-IBM-INFO-160320/201 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174342.<br>**CVE ID : CVE-2020-4162** | | |
| **Imagemagick** | | | | | |
| **imagemagick** | | | | | |
| Out-of-bounds Read | 10-03-2020 | 4.3 | In ImageMagick 7.0.9, an out-of-bounds read vulnerability exists within the ReadHEICImageByID function in coders\heic.c. It can be triggered via an image with a width or height value that exceeds the actual size of the image.<br>**CVE ID : CVE-2020-10251** | N/A | A-IMA-IMAG-160320/202 |
| **Jenkins** | | | | | |
| **skytap_cloud_ci** | | | | | |
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 4 | Jenkins Skytap Cloud CI Plugin 2.07 and earlier transmits configured credentials in plain text as part of job configuration forms, potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2157** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1522 | A-JEN-SKYT-160320/203 |
| **openshift_deployer** | | | | | |
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 5 | Jenkins OpenShift Deployer Plugin 1.2.0 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1518 | A-JEN-OPEN-160320/204 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2155** | | |
| **zephyr_enterprise_test_management** | | | | | |
| Insufficiently Protected Credentials | 09-03-2020 | 2.1 | Jenkins Zephyr Enterprise Test Management Plugin 1.9.1 and earlier stores its Zephyr password in plain text on the Jenkins master file system.<br>**CVE ID : CVE-2020-2145** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1596 | A-JEN-ZEPH-160320/205 |
| **rundeck** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 09-03-2020 | 5.5 | Jenkins Rundeck Plugin 3.6.6 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.<br>**CVE ID : CVE-2020-2144** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1702 | A-JEN-RUND-160320/206 |
| **script_security** | | | | | |
| Incorrect Authorization | 09-03-2020 | 6.5 | Sandbox protection in Jenkins Script Security Plugin 1.70 and earlier could be circumvented through crafted constructor calls and crafted constructor bodies.<br>**CVE ID : CVE-2020-2134** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1754 | A-JEN-SCRI-160320/207 |
| Incorrect Authorization | 09-03-2020 | 6.5 | Sandbox protection in Jenkins Script Security Plugin 1.70 and earlier could be circumvented through crafted method calls on objects that implement GroovyInterceptable.<br>**CVE ID : CVE-2020-2135** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1754 | A-JEN-SCRI-160320/208 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **git** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 3.5 | 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.<br>**CVE ID : CVE-2020-2136** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1723 | A-JEN-GIT-160320/209 |
| **repository_connector** | | | | | |
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 5 | Jenkins Repository Connector Plugin 1.2.6 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2149** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1520 | A-JEN-REPO-160320/210 |
| **timestamper** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 3.5 | Jenkins Timestamper Plugin 1.11.1 and earlier does not sanitize HTML formatting of its output, resulting in a stored XSS vulnerability exploitable by attackers with Overall/Administer permission.<br>**CVE ID : CVE-2020-2137** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1784 | A-JEN-TIME-160320/211 |
| **cobertura** | | | | | |
| Improper Restriction of XML External Entity | 09-03-2020 | 5.5 | Jenkins Cobertura Plugin 1.15 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. | https://jenkins.io/security/advisory/2020-03-09/#SECURI | A-JEN-COBE-160320/212 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Reference ('XXE') | | | **CVE ID : CVE-2020-2138** | TY-1700 | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 09-03-2020 | 8.5 | An arbitrary file write vulnerability in Jenkins Cobertura Plugin 1.15 and earlier allows attackers able to control the coverage report file contents to overwrite any file on the Jenkins master file system.<br>**CVE ID : CVE-2020-2139** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1668 | A-JEN-COBE-160320/213 |
| **audit_trail** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 4.3 | Jenkins Audit Trail Plugin 3.2 and earlier does not escape the error message for the URL Patterns field form validation, resulting in a reflected cross-site scripting vulnerability.<br>**CVE ID : CVE-2020-2140** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1722 | A-JEN-AUDI-160320/214 |
| **p4** | | | | | |
| Cross-Site Request Forgery (CSRF) | 09-03-2020 | 4.3 | A cross-site request forgery vulnerability in Jenkins P4 Plugin 1.10.10 and earlier allows attackers to trigger builds or add a labels in Perforce.<br>**CVE ID : CVE-2020-2141** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1765 | A-JEN-P4-160320/215 |
| Missing Authorization | 09-03-2020 | 4 | A missing permission check in Jenkins P4 Plugin 1.10.10 and earlier allows attackers with Overall/Read permission to trigger builds.<br>**CVE ID : CVE-2020-2142** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1765 | A-JEN-P4-160320/216 |
| **logstash** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 5 | Jenkins Logstash Plugin 2.3.1 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2143** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1516 | A-JEN-LOGS-160320/217 |
| **mac** | | | | | |
| Improper Verification of Cryptographic Signature | 09-03-2020 | 5.8 | Jenkins Mac Plugin 1.1.0 and earlier does not validate SSH host keys when connecting agents created by the plugin, enabling man-in-the-middle attacks.<br>**CVE ID : CVE-2020-2146** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1692 | A-JEN-MAC-160320/218 |
| Cross-Site Request Forgery (CSRF) | 09-03-2020 | 4.3 | A cross-site request forgery vulnerability in Jenkins Mac Plugin 1.1.0 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials.<br>**CVE ID : CVE-2020-2147** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1761 | A-JEN-MAC-160320/219 |
| Incorrect Authorization | 09-03-2020 | 4 | A missing permission check in Jenkins Mac Plugin 1.1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified SSH server using attacker-specified credentials.<br>**CVE ID : CVE-2020-2148** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1761 | A-JEN-MAC-160320/220 |
| **sonar_quality_gates** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 5 | Jenkins Sonar Quality Gates Plugin 1.3.1 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2150** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1523 | A-JEN-SONA-160320/221 |
| **quality_gates** | | | | | |
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 5 | Jenkins Quality Gates Plugin 2.5 and earlier transmits configured credentials in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2151** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1519 | A-JEN-QUAL-160320/222 |
| **subversion_release_manager** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 4.3 | Jenkins Subversion Release Manager Plugin 1.2 and earlier does not escape the error message for the Repository URL field form validation, resulting in a reflected cross-site scripting vulnerability.<br>**CVE ID : CVE-2020-2152** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1727 | A-JEN-SUBV-160320/223 |
| **backlog** | | | | | |
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 4 | Jenkins Backlog Plugin 2.4 and earlier transmits configured credentials in plain text as part of job configuration forms, potentially resulting in | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1510 | A-JEN-BACK-160320/224 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | their exposure.<br>**CVE ID : CVE-2020-2153** | | |
| **zephyr_for_jira_test_management** | | | | | |
| Cleartext Storage of Sensitive Information | 09-03-2020 | 2.1 | Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier stores its credentials in plain text in a global configuration file on the Jenkins master file system.<br>**CVE ID : CVE-2020-2154** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1550 | A-JEN-ZEPH-160320/225 |
| **literate** | | | | | |
| Deserialization of Untrusted Data | 09-03-2020 | 6.5 | Jenkins Literate Plugin 1.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.<br>**CVE ID : CVE-2020-2158** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1750 | A-JEN-LITE-160320/226 |
| **cryptomove** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 09-03-2020 | 9 | Jenkins CryptoMove Plugin 0.1.33 and earlier allows attackers with Job/Configure access to execute arbitrary OS commands on the Jenkins master as the OS user account running Jenkins.<br>**CVE ID : CVE-2020-2159** | https://jenkins.io/security/advisory/2020-03-09/#SECURITY-1635 | A-JEN-CRYP-160320/227 |
| **deployhub** | | | | | |
| Cleartext Transmission of Sensitive Information | 09-03-2020 | 4 | Jenkins DeployHub Plugin 8.0.14 and earlier transmits configured credentials in plain text as part of job configuration | https://jenkins.io/security/advisory/2020-03-09/#SECURI | A-JEN-DEPL-160320/228 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | forms, potentially resulting in their exposure.<br>**CVE ID : CVE-2020-2156** | TY-1511 | |
| **Johnsoncontrols** | | | | | |
| **metasys_application_and_data_server** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | A-JOH-META-160320/229 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **metasys_extended_application_and_data_server** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | A-JOH-META-160320/230 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **metasys_lonworks_control_server** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | A-JOH-META-160320/231 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **metasys_open_application_server** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | A-JOH-META-160320/232 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **metasys_open_data_server** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | A-JOH-META-160320/233 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **metasys_system_configuration_tool** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | A-JOH-META-160320/234 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **jpaseto_project** | | | | | |
| **jpaseto** | | | | | |
| Inadequate Encryption Strength | 09-03-2020 | 5 | JPaseto before 0.3.0 generates weak hashes when using v2.local tokens.<br>**CVE ID : CVE-2020-10244** | https://github.com/paseto-toolkit/jpaseto/releases/tag/jpaseto-0.3.0 | A-JPA-JPAS-160320/235 |
| **Knowledgebase-script** | | | | | |
| **phpkb** | | | | | |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 3.5 | The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or | N/A | A-KNO-PHPK-160320/236 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | HTML) in admin/report-referrers.php by adding a question mark (?) followed by the payload.<br>**CVE ID : CVE-2020-10448** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10476** | N/A | A-KNO-PHPK-160320/237 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 3.5 | Reflected XSS in admin/manage-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.<br>**CVE ID : CVE-2020-10477** | N/A | A-KNO-PHPK-160320/238 |
| **Linuxfoundation** | | | | | |
| **dojo** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 10-03-2020 | 5 | In affected versions of dojo (NPM package), the deepCopy method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or | https://github.com/dojo/dojo/security/advisories/GHSA-jxfh-8wgv-vfr2 | A-LIN-DOJO-160320/239 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pollute, a JavaScript application object prototype of the base object by injecting other values. This has been patched in versions 1.12.8, 1.13.7, 1.14.6, 1.15.3 and 1.16.2<br>**CVE ID : CVE-2020-5258** | | |
| **dojox** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 10-03-2020 | 5 | In affected versions of dojox (NPM package), the jqMix method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values. This has been patched in versions 1.11.10, 1.12.8, 1.13.7, 1.14.6, 1.15.3 and 1.16.2<br>**CVE ID : CVE-2020-5259** | https://github.com/dojo/dojox/security/advisories/GHSA-3hw5-q855-g6cw | A-LIN-DOJO-160320/240 |
| **Livezilla** | | | | | |
| **livezilla** | | | | | |
| Improper Neutralization of Input During Web Page | 09-03-2020 | 4.3 | An issue was discovered in chat.php in LiveZilla Live Chat 8.0.1.3 (Helpdesk). A blind JavaScript injection lies in the name | N/A | A-LIV-LIVE-160320/241 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | parameter. Triggering this can fetch the username and passwords of the helpdesk employees in the URI. This leads to a privilege escalation, from unauthenticated to user-level access, leading to full account takeover. The attack fetches multiple credentials because they are stored in the database (stored XSS). This affects the mobile/chat URI via the lgn and psswrd parameters.<br>**CVE ID : CVE-2020-9758** | | |
| **Mahara** | | | | | |
| **mahara** | | | | | |
| Information Exposure | 09-03-2020 | 4 | In Mahara 18.10 before 18.10.5, 19.04 before 19.04.4, and 19.10 before 19.10.2, certain personal information is discoverable inspecting network responses on the 'Edit access' screen when sharing portfolios.<br>**CVE ID : CVE-2020-9282** | https://mahara.org/interaction/forum/topic.php?id=8590 | A-MAH-MAHA-160320/242 |
| Information Exposure | 09-03-2020 | 4 | In Mahara 18.10 before 18.10.5, 19.04 before 19.04.4, and 19.10 before 19.10.2, file metadata information is disclosed to group members in the Elasticsearch result list despite them not having access to that artefact anymore. | https://mahara.org/interaction/forum/topic.php?id=8589 | A-MAH-MAHA-160320/243 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-9386** | | |
| **Metalgenix** | | | | | |
| **genixcms** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-03-2020 | 6.8 | GeniXCMS 1.1.7 is vulnerable to user privilege escalation due to broken access control. This issue exists because of an incomplete fix for CVE-2015-2680, in which "token" is used as a CSRF protection mechanism, but without validation that "token" is associated with an administrative user.<br>**CVE ID : CVE-2020-10057** | N/A | A-MET-GENI-160320/244 |
| **Microfocus** | | | | | |
| **service_manager** | | | | | |
| URL Redirection to Untrusted Site ('Open Redirect') | 09-03-2020 | 4.9 | There is an improper restriction of rendered UI layers or frames vulnerability in Micro Focus Service Manager Release Control versions 9.50 and 9.60. The vulnerability may result in the ability of malicious users to perform UI redress attacks.<br>**CVE ID : CVE-2020-9517** | https://softwaresupport.softwaregrp.com/doc/KM03604692 | A-MIC-SERV-160320/245 |
| **Microsoft** | | | | | |
| **application_inspector** | | | | | |
| Improper Neutralization of Input During Web Page Generation | 12-03-2020 | 6.8 | A remote code execution vulnerability exists in Application Inspector version v1.0.23 or earlier when the tool reflects example code snippets | N/A | A-MIC-APPL-160320/246 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | from third-party source files into its HTML output, aka 'Remote Code Execution Vulnerability in Application Inspector'.<br>**CVE ID : CVE-2020-0872** | | |
| **Misp** | | | | | |
| **misp** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 4.3 | MISP 2.4.122 has reflected XSS via unsanitized URL parameters. This is related to app/View/Users/statistics_orgs.ctp.<br>**CVE ID : CVE-2020-10246** | N/A | A-MIS-MISP-160320/247 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 4.3 | MISP 2.4.122 has Persistent XSS in the sighting popover tool. This is related to app/View/Elements/Events/View/sighting_field.ctp.<br>**CVE ID : CVE-2020-10247** | N/A | A-MIS-MISP-160320/248 |
| **Monstra** | | | | | |
| **monstra** | | | | | |
| Missing Authorization | 07-03-2020 | 4 | Monstra CMS through 3.0.4 allows remote authenticated users to take over arbitrary user accounts via a modified login parameter to an edit URI, as demonstrated by login=victim to the users/21/edit URI.<br>**CVE ID : CVE-2020-8439** | N/A | A-MON-MONS-160320/249 |
| **Mozilla** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **firefox** | | | | | |
| Out-of-bounds Write | 02-03-2020 | 6.8 | A content process could have modified shared memory relating to crash reporting information, crash itself, and cause an out-of-bound write. This could have caused memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 73 and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6796** | N/A | A-MOZ-FIRE-160320/250 |
| Improper Input Validation | 02-03-2020 | 4.3 | By downloading a file with the .fileloc extension, a semi-privileged extension could launch an arbitrary application on the user's computer. The attacker is restricted as they are unable to download non-quarantined files or supply command line arguments to the application, limiting the impact. Note: this issue only occurs on Mac OSX. Other operating systems are unaffected. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6797** | N/A | A-MOZ-FIRE-160320/251 |
| Improper Neutralization of Input During Web Page Generation | 02-03-2020 | 4.3 | If a template tag was used in a select tag, the parser could be confused and allow JavaScript parsing and execution when it should not be allowed. A | N/A | A-MOZ-FIRE-160320/252 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | site that relied on the browser behaving correctly could suffer a cross-site scripting vulnerability as a result. In general, this flaw cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but is potentially a risk in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6798** | | |
| Improper Input Validation | 02-03-2020 | 5.1 | Command line arguments could have been injected during Firefox invocation as a shell handler for certain unsupported file types. This required Firefox to be configured as the default handler for a given file type and for a file downloaded to be opened in a third party application that insufficiently sanitized URL data. In that situation, clicking a link in the third party application could have been used to retrieve and execute files whose location was supplied through command line arguments. Note: This issue only affects Windows operating systems and when Firefox | N/A | A-MOZ-FIRE-160320/253 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | is configured as the default handler for non-default filetypes. Other operating systems are unaffected. This vulnerability affects Firefox < 73 and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6799** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 02-03-2020 | 6.8 | Mozilla developers and community members reported memory safety bugs present in Firefox 72 and Firefox ESR 68.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6800** | N/A | A-MOZ-FIRE-160320/254 |
| Improper Restriction of Operations within the Bounds of a | 02-03-2020 | 6.8 | Mozilla developers reported memory safety bugs present in Firefox 72. Some of these bugs showed evidence of memory corruption and | N/A | A-MOZ-FIRE-160320/255 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Memory Buffer | | | we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 73.<br>**CVE ID : CVE-2020-6801** | | |
| **firefox_esr** | | | | | |
| Out-of-bounds Write | 02-03-2020 | 6.8 | A content process could have modified shared memory relating to crash reporting information, crash itself, and cause an out-of-bound write. This could have caused memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 73 and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6796** | N/A | A-MOZ-FIRE-160320/256 |
| Improper Input Validation | 02-03-2020 | 4.3 | By downloading a file with the .fileloc extension, a semi-privileged extension could launch an arbitrary application on the user's computer. The attacker is restricted as they are unable to download non-quarantined files or supply command line arguments to the application, limiting the impact. Note: this issue only occurs on Mac OSX. Other operating systems are unaffected. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < | N/A | A-MOZ-FIRE-160320/257 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ESR68.5.<br>**CVE ID : CVE-2020-6797** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-03-2020 | 4.3 | If a template tag was used in a select tag, the parser could be confused and allow JavaScript parsing and execution when it should not be allowed. A site that relied on the browser behaving correctly could suffer a cross-site scripting vulnerability as a result. In general, this flaw cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but is potentially a risk in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6798** | N/A | A-MOZ-FIRE-160320/258 |
| Improper Input Validation | 02-03-2020 | 5.1 | Command line arguments could have been injected during Firefox invocation as a shell handler for certain unsupported file types. This required Firefox to be configured as the default handler for a given file type and for a file downloaded to be opened in a third party application that insufficiently sanitized URL data. In that situation, clicking a link in | N/A | A-MOZ-FIRE-160320/259 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the third party application could have been used to retrieve and execute files whose location was supplied through command line arguments. Note: This issue only affects Windows operating systems and when Firefox is configured as the default handler for non-default filetypes. Other operating systems are unaffected. This vulnerability affects Firefox < 73 and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6799** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 02-03-2020 | 6.8 | Mozilla developers and community members reported memory safety bugs present in Firefox 72 and Firefox ESR 68.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < | N/A | A-MOZ-FIRE-160320/260 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ESR68.5.<br>**CVE ID : CVE-2020-6800** | | |
| **thunderbird** | | | | | |
| Missing Initialization of Resource | 02-03-2020 | 4.3 | When deriving an identifier for an email message, uninitialized memory was used in addition to the message contents. This vulnerability affects Thunderbird < 68.5.<br>**CVE ID : CVE-2020-6792** | N/A | A-MOZ-THUN-160320/261 |
| Out-of-bounds Read | 02-03-2020 | 4.3 | When processing an email message with an ill-formed envelope, Thunderbird could read data from a random memory location. This vulnerability affects Thunderbird < 68.5.<br>**CVE ID : CVE-2020-6793** | N/A | A-MOZ-THUN-160320/262 |
| Insufficiently Protected Credentials | 02-03-2020 | 4.3 | If a user saved passwords before Thunderbird 60 and then later set a master password, an unencrypted copy of these passwords is still accessible. This is because the older stored password file was not deleted when the data was copied to a new format starting in Thunderbird 60. The new master password is added only on the new file. This could allow the exposure of stored password data outside of user expectations. This vulnerability affects | N/A | A-MOZ-THUN-160320/263 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Thunderbird < 68.5.<br>**CVE ID : CVE-2020-6794** | | |
| NULL Pointer Dereference | 02-03-2020 | 4.3 | When processing a message that contains multiple S/MIME signatures, a bug in the MIME processing code caused a null pointer dereference, leading to an unexploitable crash. This vulnerability affects Thunderbird < 68.5.<br>**CVE ID : CVE-2020-6795** | N/A | A-MOZ-THUN-160320/264 |
| Improper Input Validation | 02-03-2020 | 4.3 | By downloading a file with the .fileloc extension, a semi-privileged extension could launch an arbitrary application on the user's computer. The attacker is restricted as they are unable to download non-quarantined files or supply command line arguments to the application, limiting the impact. Note: this issue only occurs on Mac OSX. Other operating systems are unaffected. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6797** | N/A | A-MOZ-THUN-160320/265 |
| Improper Neutralization of Input During Web Page Generation | 02-03-2020 | 4.3 | If a template tag was used in a select tag, the parser could be confused and allow JavaScript parsing and execution when it should not be allowed. A | N/A | A-MOZ-THUN-160320/266 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | site that relied on the browser behaving correctly could suffer a cross-site scripting vulnerability as a result. In general, this flaw cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but is potentially a risk in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6798** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 02-03-2020 | 6.8 | Mozilla developers and community members reported memory safety bugs present in Firefox 72 and Firefox ESR 68.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, | N/A | A-MOZ-THUN-160320/267 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6800** | | |
| **munkireport_project** | | | | | |
| **munkireport** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 09-03-2020 | 6.5 | An issue was discovered in MunkiReport before 5.3.0. An authenticated user could achieve SQL Injection in app/models/tablequery.php by crafting a special payload on the /datatables/data endpoint.<br>**CVE ID : CVE-2020-10190** | N/A | A-MUN-MUNK-160320/268 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 3.5 | An issue was discovered in MunkiReport before 5.3.0. An authenticated actor can send a custom XSS payload through the /module/comment/save endpoint. The payload will be executed by any authenticated users browsing the application. This concerns app/controllers/client.php:detail.<br>**CVE ID : CVE-2020-10191** | N/A | A-MUN-MUNK-160320/269 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-03-2020 | 4.3 | An issue was discovered in Munkireport before 5.3.0.3923. An unauthenticated actor can send a custom XSS payload through the /report/broken_client endpoint. The payload will be executed by any authenticated users | N/A | A-MUN-MUNK-160320/270 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | browsing the application. This concerns app/views/listings/default.php.<br>**CVE ID : CVE-2020-10192** | | |
| **Naver** | | | | | |
| **cloud_explorer** | | | | | |
| Download of Code Without Integrity Check | 03-03-2020 | 6.4 | Naver Cloud Explorer before 2.2.2.11 allows the system to download an arbitrary file from the attacker's server and execute it during the upgrade.<br>**CVE ID : CVE-2020-9751** | https://cve.naver.com/detail/cve-2020-9751 | A-NAV-CLOU-160320/271 |
| **nethack** | | | | | |
| **nethack** | | | | | |
| Improper Privilege Management | 10-03-2020 | 4.6 | NetHack before version 3.6.0 allowed malicious use of escaping of characters in the configuration file (usually .nethackrc) which could be exploited. This bug is patched in NetHack 3.6.0.<br>**CVE ID : CVE-2020-5253** | https://github.com/NetHack/NetHack/security/advisories/GHSA-2c7p-3fj4-223m | A-NET-NETH-160320/272 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-03-2020 | 4.6 | In NetHack before 3.6.6, some out-of-bound values for the hilite_status option can be exploited. NetHack 3.6.6 resolves this issue.<br>**CVE ID : CVE-2020-5254** | https://github.com/NetHack/NetHack/security/advisories/GHSA-2ch6-6r8h-m2p9 | A-NET-NETH-160320/273 |
| **netkit_telnet_project** | | | | | |
| **netkit_telnet** | | | | | |
| Buffer Copy | 06-03-2020 | 10 | utility.c in telnetd in netkit | N/A | A-NET- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| without Checking Size of Input ('Classic Buffer Overflow') | | | telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.<br>**CVE ID : CVE-2020-10188** | | NETK-160320/274 |
| **Nvidia** | | | | | |
| **geforce_experience** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.<br>**CVE ID : CVE-2020-5957** | N/A | A-NVI-GEFO-160320/275 |
| Untrusted Search Path | 11-03-2020 | 4.4 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of service, or information disclosure.<br>**CVE ID : CVE-2020-5958** | N/A | A-NVI-GEFO-160320/276 |
| **Palemoon** | | | | | |
| **pale_moon** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-03-2020 | 5 | Pale Moon 28.x before 28.8.4 has a segmentation fault related to module scripting, as demonstrated by a Lacoste web site. **CVE ID : CVE-2020-9545** | N/A | A-PAL-PALE-160320/277 |
| **parseplatform** | | | | | |
| **parse-server** | | | | | |
| Incorrect Authorization | 04-03-2020 | 5 | In parser-server before version 4.1.0, you can fetch all the users objects, by using regex in the NoSQL query. Using the NoSQL, you can use a regex on sessionToken and find valid accounts this way. **CVE ID : CVE-2020-5251** | https://github.com/parse-community/parse-server/security/advisories/GHSA-h4mf-75hf-67w4 | A-PAR-PARS-160320/278 |
| **pdfresurrect_project** | | | | | |
| **pdfresurrect** | | | | | |
| Out-of-bounds Write | 02-03-2020 | 6.8 | In PDFResurrect 0.12 through 0.19, get_type in pdf.c has an out-of-bounds write via a crafted PDF document. **CVE ID : CVE-2020-9549** | N/A | A-PDF-PDFR-160320/279 |
| **phpgurukul** | | | | | |
| **daily_expense_tracker_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-03-2020 | 7.5 | PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to SQL injection, as demonstrated by the email parameter in index.php or register.php. The SQL injection allows to dump the MySQL database and to bypass the login prompt. | N/A | A-PHP-DAIL-160320/280 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10106** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-03-2020 | 3.5 | PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS, as demonstrated by the ExpenseItem or ExpenseCost parameter in manage-expense.php.<br>**CVE ID : CVE-2020-10107** | https://frostylabs.net/writeups/cve-2020-10107/ | A-PHP-DAIL-160320/281 |
| **phpgurukul_online_book_store** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 08-03-2020 | 7.5 | An unauthenticated file upload vulnerability has been identified in admin_add.php in PHPGurukul Online Book Store 1.0. The vulnerability could be exploited by an unauthenticated remote attacker to upload content to the server, including PHP files, which could result in command execution.<br>**CVE ID : CVE-2020-10224** | N/A | A-PHP-PHPG-160320/282 |
| **phpgurukul_job_portal** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 08-03-2020 | 7.5 | An unauthenticated file upload vulnerability has been identified in admin/gallery.php in PHPGurukul Job Portal 1.0. The vulnerability could be exploited by an unauthenticated remote attacker to upload content to the server, including PHP files, which could result in command execution. | N/A | A-PHP-PHPG-160320/283 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10225** | | |
| **Phpipam** | | | | | |
| **phpipam** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-03-2020 | 6.8 | An issue was discovered in tools/pass-change/result.php in phpIPAM 1.4. CSRF can be used to change the password of any user/admin, to escalate privileges, and to gain access to more data and functionality. This issue exists due to the lack of a requirement to provide the old password, and the lack of security tokens.<br>**CVE ID : CVE-2020-7988** | N/A | A-PHP-PHPI-160320/284 |
| **Pivotal** | | | | | |
| **reactor_netty** | | | | | |
| Improper Handling of Exceptional Conditions | 03-03-2020 | 5 | Reactor Netty HttpServer, versions 0.9.3 and 0.9.4, is exposed to a URISyntaxException that causes the connection to be closed prematurely instead of producing a 400 response.<br>**CVE ID : CVE-2020-5403** | https://pivotal.io/security/cve-2020-5403 | A-PIV-REAC-160320/285 |
| Insufficiently Protected Credentials | 03-03-2020 | 4.9 | The HttpClient from Reactor Netty, versions 0.9.x prior to 0.9.5, and versions 0.8.x prior to 0.8.16, may be used incorrectly, leading to a credentials leak during a redirect to a different domain. In order for this to | https://pivotal.io/security/cve-2020-5404 | A-PIV-REAC-160320/286 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | happen, the HttpClient must have been explicitly configured to follow redirects.<br>**CVE ID : CVE-2020-5404** | | |
| **Prestashop** | | | | | |
| **prestashop** | | | | | |
| Files or Directories Accessible to External Parties | 05-03-2020 | 4.9 | In PrestaShop before version 1.7.6.4, when a customer edits their address, they can freely change the id_address in the form, and thus steal someone else's address. It is the same with CustomerForm, you are able to change the id_customer and change all information of all accounts. The problem is patched in version 1.7.6.4.<br>**CVE ID : CVE-2020-5250** | https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-mhfc-6rhg-fxp3 | A-PRE-PRES-160320/287 |
| **puma** | | | | | |
| **puma** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 02-03-2020 | 4 | In Puma (RubyGem) before 4.3.3 and 3.12.4, if an application using Puma allows untrusted input in an early-hints header, an attacker can use a carriage return character to end the header and inject malicious content, such as additional headers or an entirely new response body. This vulnerability is known as HTTP Response Splitting. While not an attack in itself, response | https://github.com/puma/puma/security/advisories/GHSA-33vf-4xgg-9r58 | A-PUM-PUMA-160320/288 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | splitting is a vector for several other attacks, such as cross-site scripting (XSS). This is related to CVE-2020-5247, which fixed this vulnerability but only for regular responses. This has been fixed in 4.3.3 and 3.12.4.<br>**CVE ID : CVE-2020-5249** | | |
| **Python** | | | | | |
| **urllib3** | | | | | |
| Uncontrolled Resource Consumption | 06-03-2020 | 7.8 | The _encode_invalid_chars function in util/url.py in the urllib3 library 1.25.2 through 1.25.7 for Python allows a denial of service (CPU consumption) because of an inefficient algorithm. The percent_encodings array contains all matches of percent encodings. It is not deduplicated. For a URL of length N, the size of percent_encodings may be up to O(N). The next step (normalize existing percent-encoded bytes) also takes up to O(N) for each step, so the total time is O(N^2). If percent_encodings were deduplicated, the time to compute _encode_invalid_chars would be O(kN), where k is at most 484 ((10+6*2)^2).<br>**CVE ID : CVE-2020-7212** | N/A | A-PYT-URLL-160320/289 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **ramp** | | | | | |
| **altimeter** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 3.5 | Ramp AltitudeCDN Altimeter before 2.4.0 allows authenticated Stored XSS via the vdms/ipmapping.jsp location field to the dms/rest/services/datastore/createOrEditValueForKey URI. **CVE ID : CVE-2020-10372** | N/A | A-RAM-ALTI-160320/290 |
| **rconfig** | | | | | |
| **rconfig** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-03-2020 | 7.5 | An issue was discovered in rConfig through 3.9.4. The web interface is prone to a SQL injection via the commands.inc.php searchColumn parameter. **CVE ID : CVE-2020-10220** | N/A | A-RCO-RCON-160320/291 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 08-03-2020 | 9 | lib/ajaxHandlers/ajaxAddTemplate.php in rConfig through 3.94 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the fileName POST parameter. **CVE ID : CVE-2020-10221** | N/A | A-RCO-RCON-160320/292 |
| **Redhat** | | | | | |
| **ansible_engine** | | | | | |
| Improper Neutralization of Special Elements | 03-03-2020 | 4.6 | A flaw was found in the pipe lookup plugin of ansible. Arbitrary commands can be run, | https://bugzilla.redhat.com/show_bug.cgi?id=CVE- | A-RED-ANSI-160320/293 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | when the pipe lookup plugin uses subprocess.Popen() with shell=True, by overwriting ansible facts and the variable is not escaped by quote plugin. An attacker could take advantage and run arbitrary commands by overwriting the ansible facts.<br>**CVE ID : CVE-2020-1734** | 2020-1734 | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 09-03-2020 | 4.6 | A flaw was found in Ansible 2.7.17 and prior, 2.8.9 and prior, and 2.9.6 and prior when using the Extract-Zip function from the win_unzip module as the extracted file(s) are not checked if they belong to the destination folder. An attacker could take advantage of this flaw by crafting an archive anywhere in the file system, using a path traversal. This issue is fixed in 2.10.<br>**CVE ID : CVE-2020-1737** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1737 | A-RED-ANSI-160320/294 |
| **openshift_container_platform** | | | | | |
| Improper Privilege Management | 09-03-2020 | 4.4 | It has been found that in openshift-enterprise version 3.11 and openshift-enterprise versions 4.1 up to, including 4.3, multiple containers modify the permissions of /etc/passwd to make them modifiable by users other | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1706 | A-RED-OPEN-160320/295 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/apb-tools-container.<br>**CVE ID : CVE-2020-1706** | | |
| **ansible** | | | | | |
| Exposure of Resource to Wrong Sphere | 11-03-2020 | 4.4 | A race condition flaw was found in Ansible Engine 2.7.17 and prior, 2.8.9 and prior, 2.9.6 and prior when running a playbook with an unprivileged become user. When Ansible needs to run a module with become user, the temporary directory is created in /var/tmp. This directory is created with "umask 77 && mkdir -p <dir>"; this operation does not fail if the directory already exists and is owned by another user. An attacker could take advantage to gain control of the become user as the target directory can be retrieved by iterating '/proc/<pid>/cmdline'.<br>**CVE ID : CVE-2020-1733** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1733 | A-RED-ANSI-160320/296 |
| **openstack** | | | | | |
| Exposure of Resource to Wrong | 11-03-2020 | 4.4 | A race condition flaw was found in Ansible Engine 2.7.17 and prior, 2.8.9 and | https://bugzilla.redhat.com/show_bug | A-RED-OPEN-160320/297 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Sphere | | | prior, 2.9.6 and prior when running a playbook with an unprivileged become user. When Ansible needs to run a module with become user, the temporary directory is created in /var/tmp. This directory is created with "umask 77 && mkdir -p <dir>"; this operation does not fail if the directory already exists and is owned by another user. An attacker could take advantage to gain control of the become user as the target directory can be retrieved by iterating '/proc/<pid>/cmdline'.<br>**CVE ID : CVE-2020-1733** | .cgi?id=CVE-2020-1733 | |
| **ansible_tower** | | | | | |
| Exposure of Resource to Wrong Sphere | 11-03-2020 | 4.4 | A race condition flaw was found in Ansible Engine 2.7.17 and prior, 2.8.9 and prior, 2.9.6 and prior when running a playbook with an unprivileged become user. When Ansible needs to run a module with become user, the temporary directory is created in /var/tmp. This directory is created with "umask 77 && mkdir -p <dir>"; this operation does not fail if the directory already exists and is owned by another user. An attacker could take | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1733 | A-RED-ANSI-160320/298 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | advantage to gain control of the become user as the target directory can be retrieved by iterating '/proc/<pid>/cmdline'.<br>**CVE ID : CVE-2020-1733** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 03-03-2020 | 4.6 | A flaw was found in the pipe lookup plugin of ansible. Arbitrary commands can be run, when the pipe lookup plugin uses subprocess.Popen() with shell=True, by overwriting ansible facts and the variable is not escaped by quote plugin. An attacker could take advantage and run arbitrary commands by overwriting the ansible facts.<br>**CVE ID : CVE-2020-1734** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1734 | A-RED-ANSI-160320/299 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 09-03-2020 | 4.6 | A flaw was found in Ansible 2.7.17 and prior, 2.8.9 and prior, and 2.9.6 and prior when using the Extract-Zip function from the win_unzip module as the extracted file(s) are not checked if they belong to the destination folder. An attacker could take advantage of this flaw by crafting an archive anywhere in the file system, using a path traversal. This issue is fixed in 2.10.<br>**CVE ID : CVE-2020-1737** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1737 | A-RED-ANSI-160320/300 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **keycloak_operator** | | | | | |
| N/A | 02-03-2020 | 7.5 | A flaw was found in all versions of the Keycloak operator, before version 8.0.2,(community only) where the operator generates a random admin password when installing Keycloak, however the password remains the same when deployed to the same OpenShift namespace.<br>**CVE ID : CVE-2020-1731** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1731 | A-RED-KEYC-160320/301 |
| **cloudforms_management_engine** | | | | | |
| Exposure of Resource to Wrong Sphere | 11-03-2020 | 4.4 | A race condition flaw was found in Ansible Engine 2.7.17 and prior, 2.8.9 and prior, 2.9.6 and prior when running a playbook with an unprivileged become user. When Ansible needs to run a module with become user, the temporary directory is created in /var/tmp. This directory is created with "umask 77 && mkdir -p <dir>"; this operation does not fail if the directory already exists and is owned by another user. An attacker could take advantage to gain control of the become user as the target directory can be retrieved by iterating '/proc/<pid>/cmdline'.<br>**CVE ID : CVE-2020-1733** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1733 | A-RED-CLOU-160320/302 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **redsoftware** | | | | | |
| **pdfescape** | | | | | |
| Untrusted Search Path | 05-03-2020 | 4.4 | An untrusted search path vulnerability in the installer of PDFescape Desktop version 4.0.22 and earlier allows an attacker to gain privileges and execute code via DLL hijacking.<br>**CVE ID : CVE-2020-9418** | https://support.pdfescape.com/hc/en-us/articles/360039586551 | A-RED-PDFE-160320/303 |
| **registrationmagic** | | | | | |
| **registrationmagic** | | | | | |
| Cross-Site Request Forgery (CSRF) | 06-03-2020 | 6.8 | A CSRF vulnerability in the RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote attackers to forge requests on behalf of a site administrator to change all settings for the plugin, including deleting users, creating new roles with escalated privileges, and allowing PHP file uploads via forms.<br>**CVE ID : CVE-2020-9454** | N/A | A-REG-REGI-160320/304 |
| Improper Privilege Management | 06-03-2020 | 4 | The RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote authenticated users (with minimal privileges) to send arbitrary emails on behalf of the site via class_rm_user_services.php send_email_user_view.<br>**CVE ID : CVE-2020-9455** | N/A | A-REG-REGI-160320/305 |
| Improper | 06-03-2020 | 6.5 | In the RegistrationMagic | N/A | A-REG-REGI- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Privilege Management | | | plugin through 4.6.0.3 for WordPress, the user controller allows remote authenticated users (with minimal privileges) to elevate their privileges to administrator via class_rm_user_controller.php rm_user_edit.<br>**CVE ID : CVE-2020-9456** | | 160320/306 |
| Improper Privilege Management | 06-03-2020 | 6.5 | The RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote authenticated users (with minimal privileges) to import custom vulnerable forms and change form settings via class_rm_form_settings_controller.php, resulting in privilege escalation.<br>**CVE ID : CVE-2020-9457** | N/A | A-REG-REGI-160320/307 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 12-03-2020 | 5.5 | An issue was discovered in the RegistrationMagic plugin 4.6.0.0 for WordPress. There is SQL injection via the rm_analytics_show_form rm_form_id parameter.<br>**CVE ID : CVE-2020-8435** | N/A | A-REG-REGI-160320/308 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 12-03-2020 | 4.3 | XSS was discovered in the RegistrationMagic plugin 4.6.0.0 for WordPress via the rm_form_id, rm_tr, or form_name parameter.<br>**CVE ID : CVE-2020-8436** | N/A | A-REG-REGI-160320/309 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Privilege Management | 06-03-2020 | 6.5 | In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the export function allows remote authenticated users (with minimal privileges) to export submitted form data and settings via class_rm_form_controller.php rm_form_export.<br>**CVE ID : CVE-2020-9458** | N/A | A-REG-REGI-160320/310 |
| **SAP** | | | | | |
| **crystal_reports** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 4.6 | SAP Business Objects Business Intelligence Platform (Crystal Reports), versions- 4.1, 4.2, allows an attacker with basic authorization to inject code that can be executed by the application and thus allowing the attacker to control the behaviour of the application, leading to Remote Code Execution. Although the mode of attack is only Local, multiple applications can be impacted as a result of the vulnerability.<br>**CVE ID : CVE-2020-6208** | N/A | A-SAP-CRYS-160320/311 |
| **erp** | | | | | |
| Missing Authorization | 10-03-2020 | 5.5 | The view FIMENAV_COMPCERT in SAP ERP (MENA Certificate Management), EAPPGLO version 607, SAP_FIN versions- 618, 730 and SAP S/4HANA | N/A | A-SAP-ERP-160320/312 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (MENA Certificate Management), S4CORE versions- 100, 101, 102, 103, 104; does not have any authorization check to it due to which an attacker without an authorization group can maintain any company certificate, leading to Missing Authorization Check.<br>**CVE ID : CVE-2020-6199** | | |
| **solution_manager** | | | | | |
| Improper Authenticati on | 10-03-2020 | 7.5 | SAP Solution Manager (Diagnostics Agent), version 720, allows unencrypted connections from unauthenticated sources. This allows an attacker to control all remote functions on the Agent due to Missing Authentication Check.<br>**CVE ID : CVE-2020-6198** | N/A | A-SAP-SOLU-160320/313 |
| Missing Authenticati on for Critical Function | 10-03-2020 | 7.5 | SAP Solution Manager (User Experience Monitoring), version- 7.2, due to Missing Authentication Check does not perform any authentication for a service resulting in complete compromise of all SMDAgents connected to the Solution Manager.<br>**CVE ID : CVE-2020-6207** | N/A | A-SAP-SOLU-160320/314 |
| **netweaver** | | | | | |
| Improper Limitation of | 10-03-2020 | 6.4 | SAP NetWeaver UDDI Server (Services Registry), | N/A | A-SAP-NETW- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| a Pathname to a Restricted Directory ('Path Traversal') | | | versions- 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; allows an attacker to exploit insufficient validation of path information provided by users, thus characters representing 'traverse to parent directory' are passed through to the file APIs, leading to Path Traversal.<br>**CVE ID : CVE-2020-6203** | | 160320/315 |
| **disclosure_management** | | | | | |
| Missing Authorization | 10-03-2020 | 6.5 | SAP Disclosure Management, version 10.1, does not perform necessary authorization checks for an authenticated user, allowing access to administration accounts by a user with no roles, leading to Missing Authorization Check.<br>**CVE ID : CVE-2020-6209** | N/A | A-SAP-DISC-160320/316 |
| **treasury_and_risk_management_\(ea-finserv\)** | | | | | |
| Missing Authorization | 10-03-2020 | 4 | The selection query in SAP Treasury and Risk Management (Transaction Management) (EA-FINSERV?versions 600, 603, 604, 605, 606, 616, 617, 618, 800 and S4CORE versions 101, 102, 103, 104) returns more records than it should be when selecting and displaying the contract number, | N/A | A-SAP-TREA-160320/317 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | leading to Missing Authorization Check.<br>**CVE ID : CVE-2020-6204** | | |
| **netweaver_as_abap_business_server_pages** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 4.3 | SAP NetWeaver AS ABAP Business Server Pages (Smart Forms), SAP_BASIS versions- 7.00, 7.01, 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53, 7.54; does not sufficiently encode user controlled inputs, allowing an unauthenticated attacker to non-permanently deface or modify displayed content and/or steal authentication information of the user and/or impersonate the user and access all information with the same rights as the target user, leading to Reflected Cross Site Scripting Vulnerability.<br>**CVE ID : CVE-2020-6205** | N/A | A-SAP-NETW-160320/318 |
| **netweaver_as_abap_business_server_pages_** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 4.3 | SAP NetWeaver AS ABAP Business Server Pages (Smart Forms), SAP_BASIS versions- 7.00, 7.01, 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53, 7.54; does not sufficiently encode user controlled inputs, allowing an unauthenticated attacker to non-permanently deface or modify displayed | N/A | A-SAP-NETW-160320/319 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | content and/or steal authentication information of the user and/or impersonate the user and access all information with the same rights as the target user, leading to Reflected Cross Site Scripting Vulnerability.<br>**CVE ID : CVE-2020-6205** | | |
| **cloud_platform_integration** | | | | | |
| Cross-Site Request Forgery (CSRF) | 10-03-2020 | 4.3 | SAP Cloud Platform Integration for Data Services, version 1.0, allows user inputs to be reflected as error or warning massages. This could mislead the victim to follow malicious instructions inserted by external attackers, leading to Cross Site Request Forgery.<br>**CVE ID : CVE-2020-6206** | N/A | A-SAP-CLOU-160320/320 |
| **fiori_launchpad** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 4.3 | SAP Fiori Launchpad, versions- 753, 754, does not sufficiently encode user-controlled inputs, and hence allowing the attacker to inject the meta tag into the launchpad html using the vulnerable parameter, leading to reflected Cross-Site Scripting (XSS) vulnerability.<br>**CVE ID : CVE-2020-6210** | N/A | A-SAP-FIOR-160320/321 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **businessobjects_mobile** | | | | | |
| N/A | 10-03-2020 | 5 | SAP BusinessObjects Mobile (MobileBIService), version 4.2, allows an attacker to generate multiple requests, using which he can block all the threads resulting in a Denial of Service.<br>**CVE ID : CVE-2020-6196** | N/A | A-SAP-BUSI-160320/322 |
| **netweaver_application_server_java** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.5 | SAP NetWeaver Application Server Java (User Management Engine), versions- 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; does not sufficiently validate the LDAP data source configuration XML document accepted from an untrusted source, leading to Missing XML Validation.<br>**CVE ID : CVE-2020-6202** | N/A | A-SAP-NETW-160320/323 |
| **commerce_cloud** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 3.5 | The SAP Commerce (SmartEdit Extension), versions- 6.6, 6.7, 1808, 1811, is vulnerable to client-side angularjs template injection, a variant of Cross-Site-Scripting (XSS) that exploits the templating facilities of the angular framework.<br>**CVE ID : CVE-2020-6200** | N/A | A-SAP-COMM-160320/324 |
| Improper | 10-03-2020 | 4.3 | The SAP Commerce | N/A | A-SAP- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Input During Web Page Generation ('Cross-site Scripting') | | | (Testweb Extension), versions- 6.6, 6.7, 1808, 1811, 1905, does not sufficiently encode user-controlled inputs, due to which certain GET URL parameters are reflected in the HTTP responses without escaping/sanitization, leading to Reflected Cross Site Scripting.<br>**CVE ID : CVE-2020-6201** | | COMM-160320/325 |
| **enable_now** | | | | | |
| Insufficient Session Expiration | 10-03-2020 | 5.5 | SAP Enable Now, before version 1911, sends the Session ID cookie value in URL. This might be stolen from the browser history or log files, leading to Information Disclosure.<br>**CVE ID : CVE-2020-6178** | N/A | A-SAP-ENAB-160320/326 |
| Insufficient Session Expiration | 10-03-2020 | 2.1 | SAP Enable Now, before version 1908, does not invalidate session tokens in a timely manner. The Insufficient Session Expiration may allow attackers with local access, for instance, to still download the portables.<br>**CVE ID : CVE-2020-6197** | N/A | A-SAP-ENAB-160320/327 |
| **treasury_and_risk_management_\(s4core\)** | | | | | |
| Missing Authorization | 10-03-2020 | 4 | The selection query in SAP Treasury and Risk Management (Transaction Management) (EA-FINSERV?versions 600, 603, 604, 605, 606, 616, | N/A | A-SAP-TREA-160320/328 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 617, 618, 800 and S4CORE versions 101, 102, 103, 104) returns more records than it should be when selecting and displaying the contract number, leading to Missing Authorization Check.<br>**CVE ID : CVE-2020-6204** | | |
| **Siemens** | | | | | |
| **spectrum_power_5** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 4.3 | A vulnerability has been identified in Spectrum Power™ 5 (All versions < v5.50 HF02). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. If deployed according to recommended system configuration, Siemens consideres the environmental vector as CR:L/IR:M/AR:H/MAV:A (4.1).<br>**CVE ID : CVE-2020-7579** | N/A | A-SIE-SPEC-160320/329 |
| **Sleuthkit** | | | | | |
| **the_sleuth_kit** | | | | | |
| Out-of-bounds Write | 09-03-2020 | 7.5 | In version 4.8.0 and earlier of The Sleuth Kit (TSK), there is a stack buffer overflow vulnerability in the YAFFS file timestamp parsing logic in | N/A | A-SLE-THE_-160320/330 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | yaffsfs_istat() in fs/yaffs.c.<br>**CVE ID : CVE-2020-10232** | | |
| Out-of-bounds Read | 09-03-2020 | 6.4 | In version 4.8.0 and earlier of The Sleuth Kit (TSK), there is a heap-based buffer over-read in ntfs_dinode_lookup in fs/ntfs.c.<br>**CVE ID : CVE-2020-10233** | N/A | A-SLE-THE_-160320/331 |
| **Sophos** | | | | | |
| **hitmanpro.alert** | | | | | |
| Improper Privilege Management | 02-03-2020 | 4.6 | Sophos HitmanPro.Alert before build 861 allows local elevation of privilege.<br>**CVE ID : CVE-2020-9540** | N/A | A-SOP-HITM-160320/332 |
| **substack** | | | | | |
| **minimist** | | | | | |
| Improper Input Validation | 11-03-2020 | 7.5 | minimist before 1.2.2 could be tricked into adding or modifying properties of Object.prototype using a "constructor" or "__proto__" payload.<br>**CVE ID : CVE-2020-7598** | N/A | A-SUB-MINI-160320/333 |
| **tecrail** | | | | | |
| **responsive_filemanager** | | | | | |
| Server-Side Request Forgery (SSRF) | 07-03-2020 | 7.5 | upload.php in Responsive FileManager 9.13.4 and 9.14.0 allows SSRF via the url parameter because file-extension blocking is mishandled and because it is possible for a DNS hostname to resolve to an internal IP address. For example, an SSRF attempt | N/A | A-TEC-RESP-160320/334 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may succeed if a .ico filename is added to the PATH_INFO. Also, an attacker could create a DNS hostname that resolves to the 0.0.0.0 IP address for DNS pinning. NOTE: this issue exists because of an incomplete fix for CVE-2018-14728.<br>**CVE ID : CVE-2020-10212** | | |
| **themerex** | | | | | |
| **fc_united-football** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-FC_U-160320/335 |
| **bugster-pests_control** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest- | N/A | A-THE-BUGS-160320/336 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **rumble-single_fighter_boxer\,_news\,_gym\,_store** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-RUMB-160320/337 |
| **tacticool-shooting_range_wordpress_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-TACT-160320/338 |
| **coinpress-cryptocurrency_magazine_\&_blog_wordpress_theme** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-COIN-160320/339 |
| **vihara-ashram\,_buddhist** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-VIHA-160320/340 |
| **katelyn-gutenberg_wordpress_blog_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions | N/A | A-THE-KATE-160320/341 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **heaven_11-multiskin_property_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-HEAV-160320/342 |
| **especio-food_gutenberg_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter. | N/A | A-THE-ESPE-160320/343 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10257** | | |
| **partiso_electioncampaign** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-PART-160320/344 |
| **kargo-freight_transport** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-KARG-160320/345 |
| **maxify-startup_blog** | | | | | |
| Improper Control of Generation of Code ('Code | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_lay | N/A | A-THE-MAXI-160320/346 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | out REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **lingvico-language_learning_school** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-LING-160320/347 |
| **aldo-gutenberg_wordpress_blog_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_lay | N/A | A-THE-ALDO-160320/348 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | out with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **vixus-startup_\/_mobile_application** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-VIXU-160320/349 |
| **wellspring_water_filter_systems** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-WELL-160320/350 |
| **nazareth-church** | | | | | |
| Improper Control of | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 | N/A | A-THE-NAZA- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation of Code ('Code Injection') | | | for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | 160320/351 |
| **tediss-soft_play_area\,_cafe_\&_child_care_center** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-TEDI-160320/352 |
| **yolox-startup_magazine_\&_blog_wordpress_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because | N/A | A-THE-YOLO-160320/353 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **meals_and_wheels-food_truck** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-MEAL-160320/354 |
| **rosalinda-vegetarian_\&_health_coach** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-ROSA-160320/355 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **vapester** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-VAPE-160320/356 |
| **modern_housewife-housewife_and_family_blog** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-MODE-160320/357 |
| **chainpress** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, | N/A | A-THE-CHAI-160320/358 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **justitia-multiskin_lawyer_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-JUST-160320/359 |
| **hobo_digital_nomad_blog** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc | N/A | A-THE-HOBO-160320/360 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **rhodos-creative_corporate_wordpress_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-RHOD-160320/361 |
| **buzz_stone-magazine_\&_blog** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-BUZZ-160320/362 |
| **corredo_sport_event** | | | | | |
| Improper Control of Generation | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access | N/A | A-THE-CORR-160320/363 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Code ('Code Injection') | | | control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **savejulia_personal_fundraising_campaign** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-SAVE-160320/364 |
| **bonkozoo_zoo** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest- | N/A | A-THE-BONK-160320/365 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **renewal-plastic_surgeon_clinic** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-RENE-160320/366 |
| **gloss_blog** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-GLOS-160320/367 |
| **plumbing-repair\,_building_\&_construction_wordpress_theme** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-PLUM-160320/368 |
| **topper_theme_and_skins** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-TOPP-160320/369 |
| **addons** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions | N/A | A-THE-ADDO-160320/370 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **ozeum-museum** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-OZEU-160320/371 |
| **chit_club-board_games** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter. | N/A | A-THE-CHIT-160320/372 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10257** | | |
| **yottis-simple_portfolio** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-YOTT-160320/373 |
| **helion-agency_\&portfolio** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-HELI-160320/374 |
| **amuli** | | | | | |
| Improper Control of Generation of Code ('Code | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_lay | N/A | A-THE-AMUL-160320/375 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | out REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **nelson-barbershop_\+_tattoo_salon** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-NELS-160320/376 |
| **hallelujah-church** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_lay | N/A | A-THE-HALL-160320/377 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | out with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **right_way** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-RIGH-160320/378 |
| **prider-pride_fest** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-PRID-160320/379 |
| **mystik-esoterics** | | | | | |
| Improper Control of | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 | N/A | A-THE-MYST- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation of Code ('Code Injection') | | | for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | 160320/380 |
| **skydiving_and_flying_company** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-SKYD-160320/381 |
| **dronex-aerial_photography_services** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because | N/A | A-THE-DRON-160320/382 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **samadhi-buddhist** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-SAMA-160320/383 |
| **tantum-rent_a_car\,_rent_a_bike\,_rent_a_scooter_multiskin_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-TANT-160320/384 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **scientia-public_library** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-SCIE-160320/385 |
| **blabber** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-BLAB-160320/386 |
| **impacto_patronus_multi-landing** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, | N/A | A-THE-IMPA-160320/387 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **rare_radio** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-RARE-160320/388 |
| **piqes-creative_startup_\&_agency_wordpress_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc | N/A | A-THE-PIQE-160320/389 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **kratz-digital_agency** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-KRAT-160320/390 |
| **pixefy** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-PIXE-160320/391 |
| **netmix-broadband_\&_telecom** | | | | | |
| Improper Control of Generation | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access | N/A | A-THE-NETM-160320/392 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Code ('Code Injection') | | | control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **kids_care** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-KIDS-160320/393 |
| **briny-diving_wordpress_theme** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest- | N/A | A-THE-BRIN-160320/394 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | | |
| **tornados** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-TORN-160320/395 |
| **gridiron** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-GRID-160320/396 |
| **yungen-digital\/marketing_agency** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Control of Generation of Code ('Code Injection') | 10-03-2020 | 7.5 | The ThemeREX Addons plugin before 2020-03-09 for WordPress lacks access control on the /trx_addons/v2/get/sc_layout REST API endpoint, allowing for PHP functions to be executed by any users, because includes/plugin.rest-api.php calls trx_addons_rest_get_sc_layout with an unsafe sc parameter.<br>**CVE ID : CVE-2020-10257** | N/A | A-THE-YUNG-160320/397 |
| **Tibco** | | | | | |
| **spotfire_analytics_platform_for_aws** | | | | | |
| Incorrect Default Permissions | 11-03-2020 | 9 | The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker with write permissions to the Spotfire Library, but not "Script Author" group permission, to modify attributes of files and objects saved to the library such that the system treats them as trusted. This could allow an attacker to cause the Spotfire Web Player, Analyst clients, and TERR Service into executing arbitrary code with the privileges of the system | http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2020/03/tibco-security-advisory-march-11-2020-tibco-spotfire-server | A-TIB-SPOT-160320/398 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | account that started those processes. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 10.8.0 and below and TIBCO Spotfire Server: versions 7.11.9 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, and 10.3.6, versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, and 10.8.0.<br>**CVE ID : CVE-2020-9408** | | |
| **spotfire_server** | | | | | |
| Incorrect Default Permissions | 11-03-2020 | 9 | The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker with write permissions to the Spotfire Library, but not "Script Author" group permission, to modify attributes of files and objects saved to the library such that the system treats them as trusted. This could allow an attacker to cause the Spotfire Web Player, Analyst clients, and TERR Service into executing | http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2020/03/tibco-security-advisory-march-11-2020-tibco-spotfire-server | A-TIB-SPOT-160320/399 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | arbitrary code with the privileges of the system account that started those processes. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 10.8.0 and below and TIBCO Spotfire Server: versions 7.11.9 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, and 10.3.6, versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, and 10.8.0.<br>**CVE ID : CVE-2020-9408** | | |
| **timeshift_project** | | | | | |
| **timeshift** | | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 05-03-2020 | 6.9 | init_tmp in TeeJee.FileSystem.vala in Timeshift before 20.03 unsafely reuses a preexisting temporary directory in the predictable location /tmp/timeshift. It follows symlinks in this location or uses directories owned by unprivileged users. Because Timeshift also executes scripts under this location, an attacker can attempt to win a race condition to replace scripts created by Timeshift with attacker- | N/A | A-TIM-TIME-160320/400 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | controlled scripts. Upon success, an attacker-controlled script is executed with full root privileges. This logic is practically always triggered when Timeshift runs regardless of the command-line arguments used.<br>**CVE ID : CVE-2020-10174** | | |
| **twistedmatrix** | | | | | |
| **twisted** | | | | | |
| Improper Input Validation | 12-03-2020 | 7.5 | In Twisted Web through 19.10.0, there was an HTTP request splitting vulnerability. When presented with two content-length headers, it ignored the first header. When the second content-length value was set to zero, the request body was interpreted as a pipelined request.<br>**CVE ID : CVE-2020-10108** | N/A | A-TWI-TWIS-160320/401 |
| Improper Input Validation | 12-03-2020 | 7.5 | In Twisted Web through 19.10.0, there was an HTTP request splitting vulnerability. When presented with a content-length and a chunked encoding header, the content-length took precedence and the remainder of the request body was interpreted as a pipelined request.<br>**CVE ID : CVE-2020-10109** | N/A | A-TWI-TWIS-160320/402 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **unctad** | | | | | |
| **asycuda_world** | | | | | |
| Inadequate Encryption Strength | 04-03-2020 | 7.5 | An issue was discovered in UNCTAD ASYCUDA World 2001 through 2020. The Java RMI Server has an Insecure Default Configuration, leading to Java Code Execution from a remote URL because an RMI Distributed Garbage Collector method is called. **CVE ID : CVE-2020-9761** | N/A | A-UNC-ASYC-160320/403 |
| **Vmware** | | | | | |
| **spring_cloud_config** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-03-2020 | 4.3 | Spring Cloud Config, versions 2.2.x prior to 2.2.2, versions 2.1.x prior to 2.1.7, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead a directory traversal attack. **CVE ID : CVE-2020-5405** | https://pivotal.io/security/cve-2020-5405 | A-VMW-SPRI-160320/404 |
| **Webkitgtk** | | | | | |
| **webkitgtk** | | | | | |
| Improper Input Validation | 02-03-2020 | 5 | WebKitGTK through 2.26.4 and WPE WebKit through 2.26.4 (which are the versions right before 2.28.0) contains a memory corruption issue (use- | N/A | A-WEB-WEBK-160320/405 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | after-free) that may lead to arbitrary code execution. This issue has been fixed in 2.28.0 with improved memory handling.<br>**CVE ID : CVE-2020-10018** | | |
| **webspellchecker** | | | | | |
| **webspellchecker** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-03-2020 | 4.3 | A cross-site scripting (XSS) vulnerability in the WSC plugin through 5.5.7.5 for CKEditor 4 allows remote attackers to run arbitrary web script inside an IFRAME element by injecting a crafted HTML element into the editor.<br>**CVE ID : CVE-2020-9440** | N/A | A-WEB-WEBS-160320/406 |
| **Wftpserver** | | | | | |
| **wing_ftp_server** | | | | | |
| Improper Preservation of Permissions | 07-03-2020 | 7.2 | Wing FTP Server v6.2.3 for Linux, macOS, and Solaris sets insecure permissions on files modified within the HTTP file management interface, resulting in files being saved with world-readable and world-writable permissions. If a sensitive system file were edited this way, a low-privilege user may escalate privileges to root.<br>**CVE ID : CVE-2020-8634** | N/A | A-WFT-WING-160320/407 |
| Improper Privilege Management | 07-03-2020 | 7.2 | Wing FTP Server v6.2.3 for Linux, macOS, and Solaris sets insecure permissions on installation directories | N/A | A-WFT-WING-160320/408 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and configuration files. This allows local users to arbitrarily create FTP users with full privileges, and escalate privileges within the operating system by modifying system files.<br>**CVE ID : CVE-2020-8635** | | |
| Missing Encryption of Sensitive Data | 07-03-2020 | 6.9 | An issue was discovered in Wing FTP Server 6.2.5 before February 2020. Due to insecure permissions when handling session cookies, a local user may view the contents of the session and session_admin directories, which expose active session cookies within the Wing FTP HTTP interface and administration panel. These cookies may be used to hijack user and administrative sessions, including the ability to execute Lua commands as root within the administration panel.<br>**CVE ID : CVE-2020-9470** | N/A | A-WFT-WING-160320/409 |
| **whmcssmarters** | | | | | |
| **web_tv_player** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 05-03-2020 | 7.5 | IPTV Smarters WEB TV PLAYER through 2020-02-22 allows attackers to execute OS commands by uploading a script.<br>**CVE ID : CVE-2020-9380** | N/A | A-WHM-WEB_-160320/410 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **wpewebkit** | | | | | |
| **wpe_webkit** | | | | | |
| Improper Input Validation | 02-03-2020 | 5 | WebKitGTK through 2.26.4 and WPE WebKit through 2.26.4 (which are the versions right before 2.28.0) contains a memory corruption issue (use-after-free) that may lead to arbitrary code execution. This issue has been fixed in 2.28.0 with improved memory handling.<br>**CVE ID : CVE-2020-10018** | N/A | A-WPE-WPE_-160320/411 |
| **yubico** | | | | | |
| **yubikey_one_time_password_validation_server** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-03-2020 | 5 | The verify endpoint in YubiKey Validation Server before 2.40 does not check the length of SQL queries, which allows remote attackers to cause a denial of service, aka SQL injection. NOTE: this issue is potentially relevant to persons outside Yubico who operate a self-hosted OTP validation service; the issue does NOT affect YubiCloud.<br>**CVE ID : CVE-2020-10184** | N/A | A-YUB-YUBI-160320/412 |
| Authentication Bypass by Capture-replay | 05-03-2020 | 6.8 | The sync endpoint in YubiKey Validation Server before 2.40 allows remote attackers to replay an OTP. NOTE: this issue is potentially relevant to persons outside Yubico who operate a self-hosted | N/A | A-YUB-YUBI-160320/413 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | OTP validation service with a non-default configuration such as an open sync pool; the issue does NOT affect YubiCloud.<br>**CVE ID : CVE-2020-10185** | | |
| **Zammad** | | | | | |
| **Zammad** | | | | | |
| Information Exposure | 05-03-2020 | 5 | An issue was discovered in Zammad 3.0 through 3.2. It does not prevent caching of confidential data within browser memory. An attacker who either remotely compromises or obtains physical access to a user's workstation can browse the browser cache contents and obtain sensitive information. The attacker does not need to be authenticated with the application to view this information, as it would be available via the browser cache.<br>**CVE ID : CVE-2020-10096** | N/A | A-ZAM-ZAMM-160320/414 |
| Information Exposure Through an Error Message | 05-03-2020 | 5 | An issue was discovered in Zammad 3.0 through 3.2. It may respond with verbose error messages that disclose internal application or infrastructure information. This information could aid attackers in successfully exploiting other vulnerabilities.<br>**CVE ID : CVE-2020-10097** | N/A | A-ZAM-ZAMM-160320/415 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-03-2020 | 3.5 | An XSS issue was discovered in Zammad 3.0 through 3.2. Malicious code can be provided by a low-privileged user through the Email functionality. The malicious JavaScript will execute within the browser of any user who opens the Ticket with the Article created from that Email. **CVE ID : CVE-2020-10098** | N/A | A-ZAM-ZAMM-160320/416 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-03-2020 | 3.5 | An XSS issue was discovered in Zammad 3.0 through 3.2. Malicious code can be provided by a low-privileged user through the Ticket functionality in Zammad. The malicious JavaScript will execute within the browser of any user who opens the ticket or has the ticket within the Toolbar. **CVE ID : CVE-2020-10099** | N/A | A-ZAM-ZAMM-160320/417 |
| Information Exposure | 05-03-2020 | 4 | An issue was discovered in Zammad 3.0 through 3.2. It allows for users to view ticket customer details associated with specific customers. However, the application does not properly implement access controls related to this functionality. As such, users of one company are able to access ticket data from other companies. Due | N/A | A-ZAM-ZAMM-160320/418 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to the multi-tenant nature of this application, users who can access ticket details from one organization to the next allows for users to exfiltrate potentially sensitive data of other companies.<br>**CVE ID : CVE-2020-10100** | | |
| Improper Input Validation | 05-03-2020 | 5 | An issue was discovered in Zammad 3.0 through 3.2. The WebSocket server crashes when messages in non-JSON format are sent by an attacker. The message format is not properly checked and parsing errors not handled. This leads to a crash of the service process.<br>**CVE ID : CVE-2020-10101** | N/A | A-ZAM-ZAMM-160320/419 |
| Information Exposure Through Discrepancy | 05-03-2020 | 3.5 | An issue was discovered in Zammad 3.0 through 3.2. The Forgot Password functionality is implemented in a way that would enable an anonymous user to guess valid user emails. In the current implementation, the application responds differently depending on whether the input supplied was recognized as associated with a valid user. This behavior could be used as part of a two-stage automated attack. | N/A | A-ZAM-ZAMM-160320/420 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | During the first stage, an attacker would iterate through a list of account names to determine which correspond to valid accounts. During the second stage, the attacker would use a list of common passwords to attempt to brute force credentials for accounts that were recognized by the system in the first stage.<br>**CVE ID : CVE-2020-10102** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-03-2020 | 3.5 | An XSS issue was discovered in Zammad 3.0 through 3.2. Malicious code can be provided by a low-privileged user through the File Upload functionality in Zammad. The malicious JavaScript will execute within the browser of any user who opens a specially crafted link to the uploaded file with an active Zammad session.<br>**CVE ID : CVE-2020-10103** | N/A | A-ZAM-ZAMM-160320/421 |
| Information Exposure | 05-03-2020 | 4 | An issue was discovered in Zammad 3.0 through 3.2. After authentication, it transmits sensitive information to the user that may be compromised and used by an attacker to gain unauthorized access. Hashed passwords are returned to the user when | N/A | A-ZAM-ZAMM-160320/422 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | visiting a certain URL.<br>**CVE ID : CVE-2020-10104** | | |
| Information Exposure | 05-03-2020 | 5 | An issue was discovered in Zammad 3.0 through 3.2. It returns source code of static resources when submitting an OPTIONS request, rather than a GET request. Disclosure of source code allows for an attacker to formulate more precise attacks. Source code was disclosed for the file 404.html (/zammad/public/404.html)<br>**CVE ID : CVE-2020-10105** | N/A | A-ZAM-ZAMM-160320/423 |
| **Zohocorp** | | | | | |
| **manageengine_desktop_central** | | | | | |
| Deserialization of Untrusted Data | 06-03-2020 | 10 | Zoho ManageEngine Desktop Central before 10.0.474 allows remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class. This is related to the CewolfServlet and MDMLogUploaderServlet servlets.<br>**CVE ID : CVE-2020-10189** | https://www.manageengine.com/products/desktop-central/remote-code-execution-vulnerability.html | A-ZOH-MANA-160320/424 |
| Improper Restriction of XML External Entity Reference | 11-03-2020 | 7.5 | An XML external entity (XXE) vulnerability in Zoho ManageEngine Desktop Central before the 07-Mar-2020 update allows remote unauthenticated users to | https://www.manageengine.com/products/desktop-central/xxe-vulnerability. | A-ZOH-MANA-160320/425 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('XXE') | | | read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request.<br>**CVE ID : CVE-2020-8540** | html | |
| **Operating System** | | | | | |
| **Apple** | | | | | |
| **mac_os** | | | | | |
| Improper Input Validation | 02-03-2020 | 4.3 | By downloading a file with the .fileloc extension, a semi-privileged extension could launch an arbitrary application on the user's computer. The attacker is restricted as they are unable to download non-quarantined files or supply command line arguments to the application, limiting the impact. Note: this issue only occurs on Mac OSX. Other operating systems are unaffected. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6797** | N/A | O-APP-MAC_-160320/426 |
| **Cisco** | | | | | |
| **telepresence_codec_c40_firmware** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on | N/A | O-CIS-TELE-160320/427 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **telepresence_codec_c60_firmware** | | | | | |
| Improper Certificate | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the | N/A | O-CIS-TELE-160320/428 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints. | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-3155** | | |
| **telepresence_codec_c90_firmware** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have | N/A | O-CIS-TELE-160320/429 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **remote_phy_120_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 7.2 | A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.<br>**CVE ID : CVE-2020-3176** | N/A | O-CIS-REMO-160320/430 |
| **remote_phy_220_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS | 04-03-2020 | 7.2 | A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute | N/A | O-CIS-REMO-160320/431 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('OS Command Injection') | | | commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.<br>**CVE ID : CVE-2020-3176** | | |
| **remote_phy_shelf_7200_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 7.2 | A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability | N/A | O-CIS-REMO-160320/432 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.<br>**CVE ID : CVE-2020-3176** | | |
| **ios_xr** | | | | | |
| Uncontrolled Resource Consumption | 04-03-2020 | 5 | A vulnerability in the IPsec packet processor of Cisco IOS XR Software could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition for IPsec sessions to an affected device. The vulnerability is due to improper handling of packets by the IPsec packet processor. An attacker could exploit this vulnerability by sending malicious ICMP error messages to an affected device that get punted to the IPsec packet processor. A successful exploit could allow the attacker to deplete IPsec memory, resulting in all future IPsec packets to an affected device being dropped by the device. Manual intervention is required to recover from this situation.<br>**CVE ID : CVE-2020-3190** | N/A | O-CIS-IOS_-160320/433 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Citrix** | | | | | |
| **gateway_firmware** | | | | | |
| Exposure of Resource to Wrong Sphere | 06-03-2020 | 5 | Citrix Gateway 11.1, 12.0, and 12.1 allows Information Exposure Through Caching. **CVE ID : CVE-2020-10110** | N/A | O-CIT-GATE-160320/434 |
| Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') | 06-03-2020 | 5 | Citrix Gateway 11.1, 12.0, and 12.1 has an Inconsistent Interpretation of HTTP Requests. **CVE ID : CVE-2020-10111** | N/A | O-CIT-GATE-160320/435 |
| Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') | 06-03-2020 | 5.8 | Citrix Gateway 11.1, 12.0, and 12.1 allows Cache Poisoning. **CVE ID : CVE-2020-10112** | N/A | O-CIT-GATE-160320/436 |
| **commscope** | | | | | |
| **arris_tg1692a_firmware** | | | | | |
| Insufficiently Protected Credentials | 04-03-2020 | 5 | ARRIS TG1692A devices allow remote attackers to discover the administrator login name and password by reading the /login page and performing base64 decoding. **CVE ID : CVE-2020-9476** | N/A | O-COM-ARRI-160320/437 |
| **Comtrend** | | | | | |
| **vr-3033_firmware** | | | | | |
| Improper Neutralization of Special Elements | 05-03-2020 | 9 | Comtrend VR-3033 DE11-416SSG-C01_R02.A2pvI042j1.d26m devices have Multiple | N/A | O-COM-VR-3-160320/438 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | Authenticated Command Injection vulnerabilities via the ping and traceroute diagnostic pages, as demonstrated by shell metacharacters in the pingIpAddress parameter to ping.cgi.<br>**CVE ID : CVE-2020-10173** | | |
| **Dlink** | | | | | |
| **dir-825_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the wps_sta_enrollee_pin parameter in a set_sta_enrollee_pin.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10213** | N/A | O-DLI-DIR--160320/439 |
| Out-of-bounds Write | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. There is a stack-based buffer overflow in the httpd binary. It allows an authenticated user to execute arbitrary code via a POST to ntp_sync.cgi with a sufficiently long parameter ntp_server.<br>**CVE ID : CVE-2020-10214** | N/A | O-DLI-DIR--160320/440 |
| Improper Neutralization of Special | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow | N/A | O-DLI-DIR--160320/441 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an OS Command ('OS Command Injection') | | | remote attackers to execute arbitrary commands via the dns_query_name parameter in a dns_query.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10215** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the date parameter in a system_time.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10216** | N/A | O-DLI-DIR--160320/442 |
| **D-link** | | | | | |
| **dsl-2640b_firmware** | | | | | |
| Improper Authentication | 05-03-2020 | 5 | An issue was discovered on D-Link DSL-2640B E1 EU_1.01 devices. The administrative interface doesn't perform authentication checks for a firmware-update POST request. Any attacker that can access the administrative interface can install firmware of their choice.<br>**CVE ID : CVE-2020-9544** | N/A | O-D-L-DSL--160320/443 |
| **dir-615jx10_firmware** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 02-03-2020 | 6.5 | fmwlan.c on D-Link DIR-615Jx10 devices has a stack-based buffer overflow via the formWlanSetup webpage parameter when f_radius_ip1 is malformed. **CVE ID : CVE-2020-9534** | N/A | O-D-L-DIR--160320/444 |
| Out-of-bounds Write | 02-03-2020 | 6.5 | fmwlan.c on D-Link DIR-615Jx10 devices has a stack-based buffer overflow via the formWlanSetup_Wizard webpage parameter when f_radius_ip1 is malformed. **CVE ID : CVE-2020-9535** | N/A | O-D-L-DIR--160320/445 |
| **Google** | | | | | |
| **android** | | | | | |
| Out-of-bounds Write | 10-03-2020 | 7.2 | In fpc_ta_get_build_info of fpc_ta_kpi.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137014293References: N/A **CVE ID : CVE-2020-0010** | N/A | O-GOO-ANDR-160320/446 |
| Out-of-bounds Write | 10-03-2020 | 7.2 | In get_auth_result of fpc_ta_hw_auth.c, there is a possible out of bounds write due to a missing bounds check. This could | N/A | O-GOO-ANDR-160320/447 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137648045References: N/A<br>**CVE ID : CVE-2020-0011** | | |
| Out-of-bounds Write | 10-03-2020 | 7.2 | In fpc_ta_pn_get_unencrypted_image of fpc_ta_pn.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137648844<br>**CVE ID : CVE-2020-0012** | N/A | O-GOO-ANDR-160320/448 |
| Missing Authorization | 10-03-2020 | 4.6 | In WifiNetworkSuggestionsManager of WifiNetworkSuggestionsManager.java, there is a possible permission revocation due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed | N/A | O-GOO-ANDR-160320/449 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | for exploitation.Product: AndroidVersions: Android-10Android ID: A-146642727<br>**CVE ID : CVE-2020-0054** | | |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In l2c_link_process_num_completed_pkts of l2c_link.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141617601<br>**CVE ID : CVE-2020-0055** | N/A | O-GOO-ANDR-160320/450 |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In btu_hcif_connection_comp_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141619686<br>**CVE ID : CVE-2020-0056** | N/A | O-GOO-ANDR-160320/451 |
| Out-of- | 10-03-2020 | 2.1 | In btm_process_inq_results | N/A | O-GOO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Read | | | of btm_inq.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141620271<br>**CVE ID : CVE-2020-0057** | | ANDR-160320/452 |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In l2c_rcv_acl_data of l2c_main.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141745011<br>**CVE ID : CVE-2020-0058** | N/A | O-GOO-ANDR-160320/453 |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In btm_ble_batchscan_filter_track_adv_vse_cback of btm_ble_batchscan.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges | N/A | O-GOO-ANDR-160320/454 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142543524<br>**CVE ID : CVE-2020-0059** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 10-03-2020 | 2.1 | In query of SmsProvider.java and MmsSmsProvider.java, there is a possible permission bypass due to SQL injection. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143229845<br>**CVE ID : CVE-2020-0060** | N/A | O-GOO-ANDR-160320/455 |
| Missing Authorization | 10-03-2020 | 4.9 | In Pixel Recorder, there is a possible permissions bypass allowing arbitrary apps to record audio. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-145504977<br>**CVE ID : CVE-2020-0061** | N/A | O-GOO-ANDR-160320/456 |
| Information | 10-03-2020 | 5 | In Euicc, there is a possible | N/A | O-GOO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exposure | | | information disclosure due to an included test Certificate. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-143232031<br>**CVE ID : CVE-2020-0062** | | ANDR-160320/457 |
| Improper Privilege Management | 10-03-2020 | 4.4 | In SurfaceFlinger, it is possible to override UI confirmation screen protected by the TEE. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-143128911<br>**CVE ID : CVE-2020-0063** | N/A | O-GOO-ANDR-160320/458 |
| Out-of-bounds Write | 10-03-2020 | 6.9 | In the netlink driver, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-65025077 | N/A | O-GOO-ANDR-160320/459 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-0066** | | |
| Out-of-bounds Write | 10-03-2020 | 7.2 | In the ioctl handlers of the Mediatek Command Queue driver, there is a possible out of bounds write due to insufficient input sanitization and missing SELinux restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-147882143References: M-ALPS04356754<br>**CVE ID : CVE-2020-0069** | N/A | O-GOO-ANDR-160320/460 |
| N/A | 10-03-2020 | 5 | In setRequirePmfInternal of sta_network.cpp, there is a possible default value being improperly applied due to a logic error. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142797954<br>**CVE ID : CVE-2020-0083** | N/A | O-GOO-ANDR-160320/461 |
| Incorrect Authorization | 10-03-2020 | 4.6 | In several functions of NotificationManagerService.java, there are missing permission checks. This could lead to local escalation of privilege by | N/A | O-GOO-ANDR-160320/462 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | creating fake system notifications with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143339775<br>**CVE ID : CVE-2020-0084** | | |
| Incorrect Authorization | 10-03-2020 | 4.6 | In setBluetoothTethering of PanService.java, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege to activate tethering with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-134487438<br>**CVE ID : CVE-2020-0085** | N/A | O-GOO-ANDR-160320/463 |
| Information Exposure | 10-03-2020 | 1.9 | In getProcessPss of ActivityManagerService.java, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-127989044 | N/A | O-GOO-ANDR-160320/464 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-0087** | | |
| Information Exposure | 10-03-2020 | 2.1 | In the WifiConfigManager, there is a possible storage of location history which can only be deleted by triggering a factory reset. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140065828<br>**CVE ID : CVE-2020-0029** | N/A | O-GOO-ANDR-160320/465 |
| Information Exposure | 10-03-2020 | 4.7 | In triggerAugmentedAutofillLocked and related functions of Session.java, it is possible for Augmented Autofill to display sensitive information to the user inappropriately. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141703197<br>**CVE ID : CVE-2020-0031** | N/A | O-GOO-ANDR-160320/466 |
| Out-of-bounds Write | 10-03-2020 | 9.3 | In ih264d_release_display_bufs of ih264d_utils.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead | N/A | O-GOO-ANDR-160320/467 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-145364230<br>**CVE ID : CVE-2020-0032** | | |
| Out-of-bounds Write | 10-03-2020 | 7.2 | In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144351324<br>**CVE ID : CVE-2020-0033** | N/A | O-GOO-ANDR-160320/468 |
| Out-of-bounds Read | 10-03-2020 | 7.8 | In vp8_decode_frame of decodeframe.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure if error correction were turned on, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android- | N/A | O-GOO-ANDR-160320/469 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 8.0 Android-8.1Android ID: A-62458770<br>**CVE ID : CVE-2020-0034** | | |
| Information Exposure | 10-03-2020 | 4.9 | In query of TelephonyProvider.java, there is a possible access to SIM card info due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-140622024<br>**CVE ID : CVE-2020-0035** | N/A | O-GOO-ANDR-160320/470 |
| Improper Privilege Management | 10-03-2020 | 7.2 | In hasPermissions of PermissionMonitor.java, there is a possible access to restricted permissions due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144679405<br>**CVE ID : CVE-2020-0036** | N/A | O-GOO-ANDR-160320/471 |
| Out-of-bounds Read | 10-03-2020 | 7.8 | In rw_i93_sm_set_read_only | N/A | O-GOO-ANDR- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of rw_i93.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143106535<br>**CVE ID : CVE-2020-0037** | | 160320/472 |
| Out-of-bounds Read | 10-03-2020 | 7.8 | In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible read of uninitialized data due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143109193<br>**CVE ID : CVE-2020-0038** | N/A | O-GOO-ANDR-160320/473 |
| Out-of-bounds Read | 10-03-2020 | 7.8 | In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible read of uninitialized data due to a missing bounds check. This could lead to remote information disclosure with no additional | N/A | O-GOO-ANDR-160320/474 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143155861<br>**CVE ID : CVE-2020-0039** | | |
| Out-of-bounds Write | 10-03-2020 | 7.2 | In binder_transaction of binder.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-145988638References: Upstream kernel<br>**CVE ID : CVE-2020-0041** | N/A | O-GOO-ANDR-160320/475 |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In fpc_ta_hw_auth_unwrap_key of fpc_ta_hw_auth_qsee.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137649599 | N/A | O-GOO-ANDR-160320/476 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-0042** | | |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In authorize_enrol of fpc_ta_hw_auth.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137650218<br>**CVE ID : CVE-2020-0043** | N/A | O-GOO-ANDR-160320/477 |
| Out-of-bounds Read | 10-03-2020 | 2.1 | In set_nonce of fpc_ta_qc_auth.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-137650219<br>**CVE ID : CVE-2020-0044** | N/A | O-GOO-ANDR-160320/478 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-03-2020 | 6.9 | In StatsService::command of StatsService.cpp, there is possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is | N/A | O-GOO-ANDR-160320/479 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141243101<br>**CVE ID : CVE-2020-0045** | | |
| Out-of-bounds Write | 10-03-2020 | 4.6 | In DrmPlugin::releaseSecure Stops of DrmPlugin.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137284652<br>**CVE ID : CVE-2020-0046** | N/A | O-GOO-ANDR-160320/480 |
| Incorrect Authorizatio n | 10-03-2020 | 2.1 | In setMasterMute of AudioService.java, there is a missing permission check. This could lead to local silencing of audio with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-141622311<br>**CVE ID : CVE-2020-0047** | N/A | O-GOO-ANDR-160320/481 |
| Use of Uninitialized Resource | 10-03-2020 | 2.1 | In onTransact of IAudioFlinger.cpp, there is a possible stack | N/A | O-GOO-ANDR-160320/482 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information leak due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-139417189<br>**CVE ID : CVE-2020-0048** | | |
| Use of Uninitialized Resource | 10-03-2020 | 4.3 | In onReadBuffer() of StreamingSource.cpp, there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140177694<br>**CVE ID : CVE-2020-0049** | N/A | O-GOO-ANDR-160320/483 |
| Out-of-bounds Write | 10-03-2020 | 4.6 | In nfa_hciu_send_msg of nfa_hci_utils.cc, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed | N/A | O-GOO-ANDR-160320/484 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | for exploitation.Product: AndroidVersions: Android-10Android ID: A-124521372<br>**CVE ID : CVE-2020-0050** | | |
| Improper Privilege Management | 10-03-2020 | 4.4 | In onCreate of SettingsHomepageActivity, there is a possible tapjacking attack. This could lead to local escalation of privilege in Settings with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-138442483<br>**CVE ID : CVE-2020-0051** | N/A | O-GOO-ANDR-160320/485 |
| Improper Privilege Management | 10-03-2020 | 1.9 | In smsSelected of AnswerFragment.java, there is a way to send an SMS from the lock screen due to a permissions bypass. This could lead to local escalation of privilege on the lock screen with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-137102479<br>**CVE ID : CVE-2020-0052** | N/A | O-GOO-ANDR-160320/486 |
| Out-of-bounds Write | 10-03-2020 | 4.6 | In convertHidlNanDataPathInitiatorRequestToLegacy, | N/A | O-GOO-ANDR-160320/487 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and convertHidlNanDataPathIndicationResponseToLegacy of hidl_struct_util.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-143789898<br>**CVE ID : CVE-2020-0053** | | |
| **humaxdigital** | | | | | |
| **hga12r-02_firmware** | | | | | |
| Session Fixation | 05-03-2020 | 6.4 | HUMAX HGA12R-02 BRGCAA 1.1.53 devices allow Session Hijacking.<br>**CVE ID : CVE-2020-9370** | N/A | O-HUM-HGA1-160320/488 |
| Improper Authenticati on | 04-03-2020 | 5 | An issue was discovered on HUMAX HGA12R-02 BRGCAA 1.1.53 devices. A vulnerability in the authentication functionality in the web-based interface could allow an unauthenticated remote attacker to capture packets at the time of authentication and gain access to the cleartext password. An attacker could use this access to create a new user account or control the device. | N/A | O-HUM-HGA1-160320/489 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-9477** | | |
| **Johnsoncontrols** | | | | | |
| **nae55_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-NAE5-160320/490 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nie55_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-NIE5-160320/491 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nie59_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-NIE5-160320/492 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nae85_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-NAE8-160320/493 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nie85_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-NIE8-160320/494 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **ul_864_uukl_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-UL_8-160320/495 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **ord-c100-13_uuklc_firmware** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | O-JOH-ORD--160320/496 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **meinbwa** | | | | | |
| **direx-pro_firmware** | | | | | |
| Information Exposure | 09-03-2020 | 5 | BWA DiREX-Pro 1.2181 devices allow remote attackers to discover passwords via a direct request to val_users.php3.<br>**CVE ID : CVE-2020-10248** | N/A | O-MEI-DIRE-160320/497 |
| Information Exposure | 09-03-2020 | 5 | BWA DiREX-Pro 1.2181 devices allow full path disclosure via an invalid name array parameter to val_soft.php3.<br>**CVE ID : CVE-2020-10249** | N/A | O-MEI-DIRE-160320/498 |
| Improper Neutralizatio | 09-03-2020 | 10 | BWA DiREX-Pro 1.2181 devices allow remote | N/A | O-MEI-DIRE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in an OS Command ('OS Command Injection') | | | attackers to execute arbitrary OS commands via shell metacharacters in the PKG parameter to uninstall.php3.<br>**CVE ID : CVE-2020-10250** | | 160320/499 |
| **mi** | | | | | |
| **miui_firmware** | | | | | |
| Information Exposure | 06-03-2020 | 4.3 | An issue was discovered on Xiaomi MIUI V11.0.5.0.QFAEUXM devices. The export component of GetApps(com.xiaomi.mipicks) mishandles the functionality of opening other components. Attackers need to induce users to open specific web pages in a specific network environment. By jumping to the WebView component of Messaging(com.android.MMS) and loading malicious web pages, information leakage can occur. This is fixed on version: 2001122; 11.0.1.54.<br>**CVE ID : CVE-2020-9530** | N/A | O-MI-MIUI-160320/500 |
| Information Exposure | 06-03-2020 | 4.3 | An issue was discovered on Xiaomi MIUI V11.0.5.0.QFAEUXM devices. In the Web resources of GetApps(com.xiaomi.mipicks), the parameters passed in are read and executed. After reading the resource | N/A | O-MI-MIUI-160320/501 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | files, relevant components open the link of the incoming URL. Although the URL is safe and can pass security detection, the data carried in the parameters are loaded and executed. An attacker can use NFC tools to get close enough to a user's unlocked phone to cause apps to be installed and information to be leaked. This is fixed on version: 2001122.<br>**CVE ID : CVE-2020-9531** | | |
| **mdz-25-dt_firmware** | | | | | |
| Insufficiently Protected Credentials | 05-03-2020 | 7.2 | An issue was discovered on XIAOMI AI speaker MDZ-25-DT 1.34.36, and 1.40.14. Attackers can get root shell by accessing the UART interface and then they can read Wi-Fi SSID or password, read the dialogue text files between users and XIAOMI AI speaker, use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, eavesdrop on users and record what XIAOMI AI speaker hears, delete the entire XIAOMI AI speaker system, modify system files, stop voice assistant service, start the XIAOMI AI speaker's SSH service as a backdoor | N/A | O-MI-MDZ--160320/502 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-8994** | | |
| **Microsoft** | | | | | |
| **windows** | | | | | |
| Improper Input Validation | 02-03-2020 | 5.1 | Command line arguments could have been injected during Firefox invocation as a shell handler for certain unsupported file types. This required Firefox to be configured as the default handler for a given file type and for a file downloaded to be opened in a third party application that insufficiently sanitized URL data. In that situation, clicking a link in the third party application could have been used to retrieve and execute files whose location was supplied through command line arguments. Note: This issue only affects Windows operating systems and when Firefox is configured as the default handler for non-default filetypes. Other operating systems are unaffected. This vulnerability affects Firefox < 73 and Firefox < ESR68.5.<br>**CVE ID : CVE-2020-6799** | N/A | O-MIC-WIND-160320/503 |
| Untrusted Search Path | 05-03-2020 | 4.4 | An untrusted search path vulnerability in the installer of PDFescape Desktop version 4.0.22 and earlier allows an attacker to gain privileges | https://support.pdfescape.com/hc/en-us/articles/36003958655 | O-MIC-WIND-160320/504 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and execute code via DLL hijacking.<br>**CVE ID : CVE-2020-9418** | 1 | |
| Improper Privilege Management | 05-03-2020 | 4.6 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.<br>**CVE ID : CVE-2020-5957** | N/A | O-MIC-WIND-160320/505 |
| Untrusted Search Path | 11-03-2020 | 4.4 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of service, or information disclosure.<br>**CVE ID : CVE-2020-5958** | N/A | O-MIC-WIND-160320/506 |
| **windows_10** | | | | | |
| Information Exposure | 12-03-2020 | 5 | An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.<br>**CVE ID : CVE-2020-0876** | N/A | O-MIC-WIND-160320/507 |
| **windows_server_2016** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information Exposure | 12-03-2020 | 5 | An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.<br>**CVE ID : CVE-2020-0876** | N/A | O-MIC-WIND-160320/508 |
| **Nvidia** | | | | | |
| **quadro_firmware** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.<br>**CVE ID : CVE-2020-5957** | N/A | O-NVI-QUAD-160320/509 |
| Untrusted Search Path | 11-03-2020 | 4.4 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of service, or information disclosure.<br>**CVE ID : CVE-2020-5958** | N/A | O-NVI-QUAD-160320/510 |
| **tesla_firmware** | | | | | |
| Improper Privilege | 05-03-2020 | 4.6 | NVIDIA Windows GPU Display Driver, all | N/A | O-NVI-TESL-160320/511 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Management | | | versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.<br>**CVE ID : CVE-2020-5957** | | |
| Untrusted Search Path | 11-03-2020 | 4.4 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of service, or information disclosure.<br>**CVE ID : CVE-2020-5958** | N/A | O-NVI-TESL-160320/512 |
| **Omron** | | | | | |
| **plc_cj1_firmware** | | | | | |
| Uncontrolled Resource Consumption | 05-03-2020 | 7.8 | In all versions of Omron PLC CJ Series, an attacker can send a series of specific data packets within a short period, causing a service error on the PLC Ethernet module, which in turn causes a PLC service denied result.<br>**CVE ID : CVE-2020-6986** | N/A | O-OMR-PLC_-160320/513 |
| **plc_cj2_firmware** | | | | | |
| Uncontrolled Resource | 05-03-2020 | 7.8 | In all versions of Omron PLC CJ Series, an attacker | N/A | O-OMR-PLC_- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | can send a series of specific data packets within a short period, causing a service error on the PLC Ethernet module, which in turn causes a PLC service denied result.<br>**CVE ID : CVE-2020-6986** | | 160320/514 |
| **Paloaltonetworks** | | | | | |
| **pan-os** | | | | | |
| Use of Externally-Controlled Format String | 11-03-2020 | 4.6 | A format string vulnerability in the PAN-OS log daemon (logd) on Panorama allows a local authenticated user to execute arbitrary code, bypassing the restricted shell and escalating privileges. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13 on Panorama. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions. This issue is fixed in PAN-OS 8.1.13 and all later PAN-OS 8.1 versions.<br>**CVE ID : CVE-2020-1979** | https://security.paloaltonetworks.com/CVE-2020-1979 | O-PAL-PAN--160320/515 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 11-03-2020 | 7.2 | A shell command injection vulnerability in the PAN-OS CLI allows a local authenticated user to escape the restricted shell and escalate privileges. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not | https://security.paloaltonetworks.com/CVE-2020-1980 | O-PAL-PAN--160320/516 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions. This issue is fixed in PAN-OS 8.1.13, and all later versions.<br>**CVE ID : CVE-2020-1980** | | |
| Exposure of Resource to Wrong Sphere | 11-03-2020 | 7.2 | A predictable temporary filename vulnerability in PAN-OS allows local privilege escalation. This issue allows a local attacker who bypassed the restricted shell to execute commands as a low privileged user and gain root access on the PAN-OS hardware or virtual appliance. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions.<br>**CVE ID : CVE-2020-1981** | https://security.paloaltonetworks.com/CVE-2020-1981 | O-PAL-PAN--160320/517 |
| **patriotmemory** | | | | | |
| **viper_rgb_firmware** | | | | | |
| Improper Privilege Management | 06-03-2020 | 4.6 | Patriot Viper RGB Driver 1.1 and prior exposes IOCTL and allows insufficient access control. The IOCTL Codes 0x80102050 and 0x80102054 allows a local user with low privileges to read/write 1/2/4 bytes from or to an IO port. This could be leveraged in a number of ways to | N/A | O-PAT-VIPE-160320/518 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ultimately run code with elevated privileges.<br>**CVE ID : CVE-2020-9756** | | |
| **plathome** | | | | | |
| **openblocks_iot_vx2_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 8.3 | OpenBlocks IoT VX2 prior to Ver.4.0.0 (Ver.3 Series) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via unspecified vectors.<br>**CVE ID : CVE-2020-5535** | N/A | O-PLA-OPEN-160320/519 |
| Improper Authentication | 04-03-2020 | 5.8 | OpenBlocks IoT VX2 prior to Ver.4.0.0 (Ver.3 Series) allows an attacker on the same network segment to bypass authentication and to initialize the device via unspecified vectors.<br>**CVE ID : CVE-2020-5536** | N/A | O-PLA-OPEN-160320/520 |
| **rubetek** | | | | | |
| **smarthome_firmware** | | | | | |
| Cleartext Transmission of Sensitive Information | 04-03-2020 | 7.5 | Rubetek SmartHome 2020 devices use unencrypted 433 MHz communication between controllers and beacons, allowing an attacker to sniff and spoof beacon requests remotely.<br>**CVE ID : CVE-2020-9550** | N/A | O-RUB-SMAR-160320/521 |
| **sumavision** | | | | | |
| **enhanced_multimedia_router_firmware** | | | | | |
| Improper Privilege | 11-03-2020 | 7.5 | goform/formEMR30 in Sumavision Enhanced Multimedia Router (EMR) | N/A | O-SUM-ENHA- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Management | | | 3.0.4.27 allows creation of arbitrary users with elevated privileges (administrator) on a device, as demonstrated by a setString=new_user<*1*>administrator<*1*>123456 request.<br>**CVE ID : CVE-2020-10181** | | 160320/522 |
| **Suse** | | | | | |
| **linux_enterprise_server** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 02-03-2020 | 1.9 | A UNIX Symbolic Link (Symlink) Following vulnerability in chkstat of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15, SUSE Linux Enterprise Server 11 set permissions intended for specific binaries on other binaries because it erroneously followed symlinks. The symlinks can't be controlled by attackers on default systems, so exploitation is difficult. This issue affects: SUSE Linux Enterprise Server 12 permissions versions prior to 2015.09.28.1626-17.27.1. SUSE Linux Enterprise Server 15 permissions versions prior to 20181116-9.23.1. SUSE Linux Enterprise Server 11 permissions versions prior to 2013.1.7-0.6.12.1. | https://bugzilla.suse.com/show_bug.cgi?id=1163922 | O-SUS-LINU-160320/523 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-8013** | | |
| **Trendnet** | | | | | |
| **tew-632brp_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the wps_sta_enrollee_pin parameter in a set_sta_enrollee_pin.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10213** | N/A | O-TRE-TEW--160320/524 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the dns_query_name parameter in a dns_query.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10215** | N/A | O-TRE-TEW--160320/525 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the date parameter in a system_time.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also | N/A | O-TRE-TEW--160320/526 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected.<br>**CVE ID : CVE-2020-10216** | | |
| **Zyxel** | | | | | |
| **atp200_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ATP2-160320/527 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **atp500_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ATP5-160320/528 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-9054** | | |
| **atp800_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ATP8-160320/529 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **usg1100_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-USG1-160320/530 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg110_firmware** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-USG1-160320/531 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg1900_firmware** | | | | | |
| Improper | 04-03-2020 | 10 | Multiple ZyXEL network- | https://ww | O-ZYX-USG1- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | | attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute | w.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | 160320/532 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg20-vpn_firmware** | | | | | |
| Improper Neutralizatio | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) | https://www.zyxel.com/ | O-ZYX-USG2-160320/533 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in an OS Command ('OS Command Injection') | | | devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the | support/remote-code-execution-vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg20w-vpn_firmware** | | | | | |
| Improper Neutralization of Special | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware | https://www.zyxel.com/support/rem | O-ZYX-USG2-160320/534 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an OS Command ('OS Command Injection') | | | version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen | ote-code-execution-vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg210_firmware** | | | | | |
| Improper Neutralization of Special Elements | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre- | https://www.zyxel.com/support/remote-code- | O-ZYX-USG2-160320/535 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a | execution-vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg310_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command | https://www.zyxel.com/support/remote-code-execution- | O-ZYX-USG3-160320/536 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('OS Command Injection') | | | injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly | vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg40_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, | https://www.zyxel.com/support/remote-code-execution-vulnerability | O-ZYX-USG4-160320/537 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('OS Command Injection') | | | which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. | -of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg40w_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS- | O-ZYX-USG4-160320/538 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways | products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg60_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.sht | O-ZYX-USG6-160320/539 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted | ml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg60w_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-USG6-160320/540 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn100_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-VPN1-160320/541 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn300_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-VPN3-160320/542 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn50_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-VPN5-160320/543 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas326_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-NAS3-160320/544 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas520_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-NAS5-160320/545 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas540_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-NAS5-160320/546 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas542_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-NAS5-160320/547 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **atp100_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ATP1-160320/548 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg2200_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-USG2-160320/549 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn1000_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-VPN1-160320/550 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **zywall110_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ZYWA-160320/551 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **zywall310_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ZYWA-160320/552 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **zywall1100_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | O-ZYX-ZYWA-160320/553 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **Hardware** | | | | | |
| **Cisco** | | | | | |
| **telepresence_codec_c40** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration | N/A | H-CIS-TELE-160320/554 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **telepresence_codec_c60** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL | N/A | H-CIS-TELE-160320/555 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **telepresence_codec_c90** | | | | | |
| Improper Certificate Validation | 04-03-2020 | 5.8 | A vulnerability in the SSL implementation of the Cisco Intelligent Proximity solution could allow an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration endpoints if the products meet the conditions | N/A | H-CIS-TELE-160320/556 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | described in the Vulnerable Products section. The vulnerability is due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint. An attacker could exploit this vulnerability by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Depending on the configuration of the endpoint, an exploit could allow the attacker to view presentation content shared on it, modify any content being presented by the victim, or have access to call controls. This vulnerability does not affect cloud registered collaboration endpoints.<br>**CVE ID : CVE-2020-3155** | | |
| **remote_phy_120** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command | 04-03-2020 | 7.2 | A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the | N/A | H-CIS-REMO-160320/557 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('OS Command Injection') | | | underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.<br>**CVE ID : CVE-2020-3176** | | |
| **remote_phy_220** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 7.2 | A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI | N/A | H-CIS-REMO-160320/558 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.<br>**CVE ID : CVE-2020-3176** | | |
| **remote_phy_shelf_7200** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 7.2 | A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.<br>**CVE ID : CVE-2020-3176** | N/A | H-CIS-REMO-160320/559 |
| **commscope** | | | | | |
| **arris_tg1692a** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Insufficiently Protected Credentials | 04-03-2020 | 5 | ARRIS TG1692A devices allow remote attackers to discover the administrator login name and password by reading the /login page and performing base64 decoding.<br>**CVE ID : CVE-2020-9476** | N/A | H-COM-ARRI-160320/560 |
| **Comtrend** | | | | | |
| **vr-3033** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 05-03-2020 | 9 | Comtrend VR-3033 DE11-416SSG-C01_R02.A2pvI042j1.d26m devices have Multiple Authenticated Command Injection vulnerabilities via the ping and traceroute diagnostic pages, as demonstrated by shell metacharacters in the pingIpAddress parameter to ping.cgi.<br>**CVE ID : CVE-2020-10173** | N/A | H-COM-VR-3-160320/561 |
| **Dlink** | | | | | |
| **dir-825** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the wps_sta_enrollee_pin parameter in a set_sta_enrollee_pin.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10213** | N/A | H-DLI-DIR--160320/562 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. There is a stack-based buffer overflow in the httpd binary. It allows an authenticated user to execute arbitrary code via a POST to ntp_sync.cgi with a sufficiently long parameter ntp_server. **CVE ID : CVE-2020-10214** | N/A | H-DLI-DIR--160320/563 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the dns_query_name parameter in a dns_query.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected. **CVE ID : CVE-2020-10215** | N/A | H-DLI-DIR--160320/564 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the date parameter in a system_time.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected. **CVE ID : CVE-2020-10216** | N/A | H-DLI-DIR--160320/565 |
| **D-link** | | | | | |
| **dsl-2640b** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Authenticati on | 05-03-2020 | 5 | An issue was discovered on D-Link DSL-2640B E1 EU_1.01 devices. The administrative interface doesn't perform authentication checks for a firmware-update POST request. Any attacker that can access the administrative interface can install firmware of their choice. **CVE ID : CVE-2020-9544** | N/A | H-D-L-DSL--160320/566 |
| **dir-615jx10** | | | | | |
| Out-of-bounds Write | 02-03-2020 | 6.5 | fmwlan.c on D-Link DIR-615Jx10 devices has a stack-based buffer overflow via the formWlanSetup webpage parameter when f_radius_ip1 is malformed. **CVE ID : CVE-2020-9534** | N/A | H-D-L-DIR--160320/567 |
| Out-of-bounds Write | 02-03-2020 | 6.5 | fmwlan.c on D-Link DIR-615Jx10 devices has a stack-based buffer overflow via the formWlanSetup_Wizard webpage parameter when f_radius_ip1 is malformed. **CVE ID : CVE-2020-9535** | N/A | H-D-L-DIR--160320/568 |
| **humaxdigital** | | | | | |
| **hga12r-02** | | | | | |
| Session Fixation | 05-03-2020 | 6.4 | HUMAX HGA12R-02 BRGCAA 1.1.53 devices allow Session Hijacking. **CVE ID : CVE-2020-9370** | N/A | H-HUM-HGA1-160320/569 |
| Improper Authenticati | 04-03-2020 | 5 | An issue was discovered on HUMAX HGA12R-02 | N/A | H-HUM-HGA1- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on | | | BRGCAA 1.1.53 devices. A vulnerability in the authentication functionality in the web-based interface could allow an unauthenticated remote attacker to capture packets at the time of authentication and gain access to the cleartext password. An attacker could use this access to create a new user account or control the device.<br>**CVE ID : CVE-2020-9477** | | 160320/570 |
| **Johnsoncontrols** | | | | | |
| **nae55** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | H-JOH-NAE5-160320/571 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nie55** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | H-JOH-NIE5-160320/572 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nie59** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | H-JOH-NIE5-160320/573 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nae85** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | H-JOH-NAE8-160320/574 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **nie85** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | H-JOH-NIE8-160320/575 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **ul_864_uukl** | | | | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or harvesting of ASCII server files. This affects Johnson Controls' Metasys | https://www.johnsoncontrols.com/cyber-solutions/security-advisories | H-JOH-UL_8-160320/576 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | | |
| **ord-c100-13_uuklc** | | | | | |
| Improper Restriction of XML External Entity | 10-03-2020 | 6.4 | XXE vulnerability exists in the Metasys family of product Web Services which has the potential to facilitate DoS attacks or | https://www.johnsoncontrols.com/cyber-solutions/se | H-JOH-ORD--160320/577 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Reference ('XXE') | | | harvesting of ASCII server files. This affects Johnson Controls' Metasys Application and Data Server (ADS, ADS-Lite) versions 10.1 and prior; Metasys Extended Application and Data Server (ADX) versions 10.1 and prior; Metasys Open Data Server (ODS) versions 10.1 and prior; Metasys Open Application Server (OAS) version 10.1; Metasys Network Automation Engine (NAE55 only) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys Network Integration Engine (NIE55/NIE59) versions 9.0.1, 9.0.2, 9.0.3, 9.0.5, 9.0.6; Metasys NAE85 and NIE85 versions 10.1 and prior; Metasys LonWorks Control Server (LCS) versions 10.1 and prior; Metasys System Configuration Tool (SCT) versions 13.2 and prior; Metasys Smoke Control Network Automation Engine (NAE55, UL 864 UUKL/ORD-C100-13 UUKLC 10th Edition Listed) version 8.1.<br>**CVE ID : CVE-2020-9044** | curity-advisories | |
| **meinbwa** | | | | | |
| **direx-pro** | | | | | |
| Information | 09-03-2020 | 5 | BWA DiREX-Pro 1.2181 | N/A | H-MEI-DIRE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exposure | | | devices allow remote attackers to discover passwords via a direct request to val_users.php3.<br>**CVE ID : CVE-2020-10248** | | 160320/578 |
| Information Exposure | 09-03-2020 | 5 | BWA DiREX-Pro 1.2181 devices allow full path disclosure via an invalid name array parameter to val_soft.php3.<br>**CVE ID : CVE-2020-10249** | N/A | H-MEI-DIRE-160320/579 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 09-03-2020 | 10 | BWA DiREX-Pro 1.2181 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the PKG parameter to uninstall.php3.<br>**CVE ID : CVE-2020-10250** | N/A | H-MEI-DIRE-160320/580 |
| **mi** | | | | | |
| **miui** | | | | | |
| Information Exposure | 06-03-2020 | 4.3 | An issue was discovered on Xiaomi MIUI V11.0.5.0.QFAEUXM devices. The export component of GetApps(com.xiaomi.mipicks) mishandles the functionality of opening other components. Attackers need to induce users to open specific web pages in a specific network environment. By jumping to the WebView component of Messaging(com.android.MMS) and loading malicious | N/A | H-MI-MIUI-160320/581 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | web pages, information leakage can occur. This is fixed on version: 2001122; 11.0.1.54.<br>**CVE ID : CVE-2020-9530** | | |
| Information Exposure | 06-03-2020 | 4.3 | An issue was discovered on Xiaomi MIUI V11.0.5.0.QFAEUXM devices. In the Web resources of GetApps(com.xiaomi.mipicks), the parameters passed in are read and executed. After reading the resource files, relevant components open the link of the incoming URL. Although the URL is safe and can pass security detection, the data carried in the parameters are loaded and executed. An attacker can use NFC tools to get close enough to a user's unlocked phone to cause apps to be installed and information to be leaked. This is fixed on version: 2001122.<br>**CVE ID : CVE-2020-9531** | N/A | H-MI-MIUI-160320/582 |
| **mdz-25-dt** | | | | | |
| Insufficiently Protected Credentials | 05-03-2020 | 7.2 | An issue was discovered on XIAOMI AI speaker MDZ-25-DT 1.34.36, and 1.40.14. Attackers can get root shell by accessing the UART interface and then they can read Wi-Fi SSID or password, read the dialogue text files between | N/A | H-MI-MDZ--160320/583 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | users and XIAOMI AI speaker, use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, eavesdrop on users and record what XIAOMI AI speaker hears, delete the entire XIAOMI AI speaker system, modify system files, stop voice assistant service, start the XIAOMI AI speaker's SSH service as a backdoor<br>**CVE ID : CVE-2020-8994** | | |
| **Nvidia** | | | | | |
| **quadro** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.<br>**CVE ID : CVE-2020-5957** | N/A | H-NVI-QUAD-160320/584 |
| Untrusted Search Path | 11-03-2020 | 4.4 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of | N/A | H-NVI-QUAD-160320/585 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | service, or information disclosure.<br>**CVE ID : CVE-2020-5958** | | |
| **tesla** | | | | | |
| Improper Privilege Management | 05-03-2020 | 4.6 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.<br>**CVE ID : CVE-2020-5957** | N/A | H-NVI-TESL-160320/586 |
| Untrusted Search Path | 11-03-2020 | 4.4 | NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of service, or information disclosure.<br>**CVE ID : CVE-2020-5958** | N/A | H-NVI-TESL-160320/587 |
| **Omron** | | | | | |
| **plc_cj1** | | | | | |
| Uncontrolled Resource Consumption | 05-03-2020 | 7.8 | In all versions of Omron PLC CJ Series, an attacker can send a series of specific data packets within a short period, causing a service error on the PLC Ethernet module, | N/A | H-OMR-PLC_-160320/588 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which in turn causes a PLC service denied result.<br>**CVE ID : CVE-2020-6986** | | |
| **plc_cj2** | | | | | |
| Uncontrolled Resource Consumption | 05-03-2020 | 7.8 | In all versions of Omron PLC CJ Series, an attacker can send a series of specific data packets within a short period, causing a service error on the PLC Ethernet module, which in turn causes a PLC service denied result.<br>**CVE ID : CVE-2020-6986** | N/A | H-OMR-PLC_-160320/589 |
| **patriotmemory** | | | | | |
| **viper_rgb** | | | | | |
| Improper Privilege Management | 06-03-2020 | 4.6 | Patriot Viper RGB Driver 1.1 and prior exposes IOCTL and allows insufficient access control. The IOCTL Codes 0x80102050 and 0x80102054 allows a local user with low privileges to read/write 1/2/4 bytes from or to an IO port. This could be leveraged in a number of ways to ultimately run code with elevated privileges.<br>**CVE ID : CVE-2020-9756** | N/A | H-PAT-VIPE-160320/590 |
| **plathome** | | | | | |
| **openblocks_iot_vx2** | | | | | |
| Improper Neutralization of Special Elements used in an OS | 04-03-2020 | 8.3 | OpenBlocks IoT VX2 prior to Ver.4.0.0 (Ver.3 Series) allows an attacker on the same network segment to execute arbitrary OS | N/A | H-PLA-OPEN-160320/591 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('OS Command Injection') | | | commands with root privileges via unspecified vectors.<br>**CVE ID : CVE-2020-5535** | | |
| Improper Authenticati on | 04-03-2020 | 5.8 | OpenBlocks IoT VX2 prior to Ver.4.0.0 (Ver.3 Series) allows an attacker on the same network segment to bypass authentication and to initialize the device via unspecified vectors.<br>**CVE ID : CVE-2020-5536** | N/A | H-PLA-OPEN-160320/592 |
| **rubetek** | | | | | |
| **smarthome** | | | | | |
| Cleartext Transmissio n of Sensitive Information | 04-03-2020 | 7.5 | Rubetek SmartHome 2020 devices use unencrypted 433 MHz communication between controllers and beacons, allowing an attacker to sniff and spoof beacon requests remotely.<br>**CVE ID : CVE-2020-9550** | N/A | H-RUB-SMAR-160320/593 |
| **sumavision** | | | | | |
| **enhanced_multimedia_router** | | | | | |
| Improper Privilege Management | 11-03-2020 | 7.5 | goform/formEMR30 in Sumavision Enhanced Multimedia Router (EMR) 3.0.4.27 allows creation of arbitrary users with elevated privileges (administrator) on a device, as demonstrated by a setString=new_user<*1*>administrator<*1*>123456 request.<br>**CVE ID : CVE-2020-10181** | N/A | H-SUM-ENHA-160320/594 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Trendnet** | | | | | |
| **tew-632brp** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the wps_sta_enrollee_pin parameter in a set_sta_enrollee_pin.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10213** | N/A | H-TRE-TEW--160320/595 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the dns_query_name parameter in a dns_query.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected.<br>**CVE ID : CVE-2020-10215** | N/A | H-TRE-TEW--160320/596 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-03-2020 | 9 | An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the date parameter in a system_time.cgi POST request. TRENDnet TEW-632BRP 1.010B32 is also affected. | N/A | H-TRE-TEW--160320/597 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-10216** | | |
| **Zyxel** | | | | | |
| **atp200** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ATP2-160320/598 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2020-9054** | | |
| **atp500** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ATP5-160320/599 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **atp800** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ATP8-160320/600 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg20-vpn** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG2-160320/601 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg20w-vpn** | | | | | |
| Improper | 04-03-2020 | 10 | Multiple ZyXEL network- | https://ww | H-ZYX-USG2- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | | attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute | w.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | 160320/602 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg40** | | | | | |
| Improper Neutralizatio | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) | https://www.zyxel.com/ | H-ZYX-USG4-160320/603 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in an OS Command ('OS Command Injection') | | | devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the | support/remote-code-execution-vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg40w** | | | | | |
| Improper Neutralizatio n of Special | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware | https://ww w.zyxel.com/ support/rem | H-ZYX-USG4-160320/604 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an OS Command ('OS Command Injection') | | | version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen | ote-code-execution-vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg60** | | | | | |
| Improper Neutralization of Special Elements | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre- | https://www.zyxel.com/support/remote-code- | H-ZYX-USG6-160320/605 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a | execution-vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg60w** | | | | | |
| Improper Neutralization of Special Elements used in an OS | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command | https://www.zyxel.com/support/remote-code-execution- | H-ZYX-USG6-160320/606 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('OS Command Injection') | | | injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly | vulnerability-of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn50** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, | https://www.zyxel.com/support/remote-code-execution-vulnerability | H-ZYX-VPN5-160320/607 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('OS Command Injection') | | | which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. | -of-NAS-products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn100** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS- | H-ZYX-VPN1-160320/608 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways | products.shtml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn300** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.sht | H-ZYX-VPN3-160320/609 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted | ml | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas326** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-NAS3-160320/610 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg110** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG1-160320/611 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg210** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG2-160320/612 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg310** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG3-160320/613 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg1100** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG1-160320/614 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg1900** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG1-160320/615 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas520** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-NAS5-160320/616 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas540** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-NAS5-160320/617 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **nas542** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-NAS5-160320/618 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **atp100** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ATP1-160320/619 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **usg2200** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-USG2-160320/620 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **vpn1000** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-VPN1-160320/621 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **zywall110** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ZYWA-160320/622 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **zywall310** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ZYWA-160320/623 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |
| **zywall1100** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-03-2020 | 10 | Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the | https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml | H-ZYX-ZYWA-160320/624 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2<br>**CVE ID : CVE-2020-9054** | | |