# National Critical Information Infrastructure Protection Centre

# Common Vulnerabilities and Exposures (CVE) Report

16 - 30 Nov 2022 Vol. 09 No. 22

## Table of Content

| Vendor | Product | Page Number |
|---|---|---|
| **audinate** | dante_enabled_zoom_rooms | 28 |
| **Automattic** | crowdsignal_dashboard | 28 |
| **automotive_shop_management_system_project** | automotive_shop_management_system | 29 |
| **awplife** | event_monster | 31 |
| **backclick** | backclick | 32 |
| **backdropcms** | backdrop | 36 |
| | backdrop_cms | 36 |
| **beautiful-cookie-banner** | beautiful_cookie_consent_banner | 37 |
| **beekeeperstudio** | beekeeper-studio | 37 |
| **benbodhi** | svg_support | 38 |
| **billing_system_project** | billing_system | 39 |
| **billing_system_project_project** | billing_system_project | 39 |
| **billing_system_project_project_project** | billing_system_project | 39 |
| **blood_donor_management_system_project** | blood_donor_management_system | 40 |
| **BOA** | boa | 40 |
| **booster** | booster_for_woocommerce | 40 |
| **btcd_project** | btcd | 44 |
| **bund** | bkg_professional_ntripcaster | 45 |
| **caehealthcare** | learningspace_enterprise | 46 |
| **chameleon_project** | chameleon | 46 |
| **churchcrm** | churchcrm | 47 |
| **Ciphercoin** | contact_form_7_database_addon | 47 |
| **clevelandwebdeveloper** | spacer | 48 |
| **clogica** | seo_redirection | 48 |
| **cncf** | knative_func | 49 |
| **code-atlantic** | popup_maker | 49 |
| **codenotary** | immudb | 50 |
| **Codepeople** | appointment_booking_calendar | 52 |
| **college_management_system_project** | college_management_system | 52 |

## Common Vulnerabilities and Exposures (CVE) Report

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Vendor: 2code** | | | | | |
| **Product: wpqa_builder** | | | | | |
| Affected Version(s): * Up to (excluding) 5.9 | | | | | |
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 8.8 | The WPQA Builder WordPress plugin before 5.9 does not have CSRF check when following and unfollowing users, which could allow attackers to make logged in users perform such actions via CSRF attacks<br>**CVE ID : CVE-2022-3688** | https://wpscan.com/vulnerability/03b2c6e6-b86e-4143-a84a-7a99060c4848 | A-2CO-WPQA-121222/1 |
| **Vendor: ABB** | | | | | |
| **Product: microscada_pro_sys600** | | | | | |
| Affected Version(s): * Up to (including) 9.3 | | | | | |
| Improper Input Validation | 21-Nov-2022 | 7.8 | An input validation vulnerability exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X SYS600. An authenticated user can launch an administrator level remote code execution irrespective of the authenticated user's role.<br>**CVE ID : CVE-2022-3388** | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000123&LanguageCode=en&DocumentPartId=&Action=Launch&elqaid=4293&elqat=1 | A-ABB-MICR-121222/2 |
| Affected Version(s): 9.4 | | | | | |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 21-Nov-2022 | 7.8 | An input validation vulnerability exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X SYS600. An authenticated user can launch an administrator level remote code execution irrespective of the authenticated user's role.<br>**CVE ID : CVE-2022-3388** | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000123&LanguageCode=en&DocumentPartId=&Action=Launch&elqaid=4293&elqat=1 | A-ABB-MICR-121222/3 |
| **Vendor: accessibility_project** | | | | | |
| **Product: accessibility** | | | | | |
| Affected Version(s): * Up to (excluding) 1.0.4 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Nov-2022 | 4.8 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Accessibility plugin <= 1.0.3 on WordPress.<br>**CVE ID : CVE-2022-41643** | https://wordpress.org/plugins/accessibility/#developers, https://patchstack.com/database/vulnerability/accessibility/wordpress-accessibility-plugin-1-0-1-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve | A-ACC-ACCE-121222/4 |
| **Vendor: aerocms_project** | | | | | |
| **Product: aerocms** | | | | | |
| Affected Version(s): 0.0.1 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 29-Nov-2022 | 7.5 | AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the Search parameter. This vulnerability allows attackers to access database information.<br>**CVE ID : CVE-2022-45329** | N/A | A-AER-AERO-121222/5 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 7.5 | AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the Category parameter at \category.php. This vulnerability allows attackers to access database information.<br>**CVE ID : CVE-2022-45330** | N/A | A-AER-AERO-121222/6 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 7.5 | AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the p_id parameter at \post.php. This vulnerability allows attackers to access database information.<br>**CVE ID : CVE-2022-45331** | N/A | A-AER-AERO-121222/7 |
| Improper Neutralization of Special Elements used in an SQL Command | 22-Nov-2022 | 4.9 | AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the post_category_id parameter at \admin\includes\edit_post.php. This vulnerability allows | N/A | A-AER-AERO-121222/8 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | attackers to access database information.<br>**CVE ID : CVE-2022-45529** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 4.9 | AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the edit parameter at \admin\categories.php. This vulnerability allows attackers to access database information.<br>**CVE ID : CVE-2022-45535** | N/A | A-AER-AERO-121222/9 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 4.9 | AeroCMS v0.0.1 was discovered to contain a SQL Injection vulnerability via the id parameter at \admin\post_comments.php. This vulnerability allows attackers to access database information.<br>**CVE ID : CVE-2022-45536** | N/A | A-AER-AERO-121222/10 |
| **Vendor: agilelogix** | | | | | |
| **Product: store_locator** | | | | | |
| Affected Version(s): * Up to (excluding) 1.4.6 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 6.1 | Cross-Site Scripting (XSS) via Cross-Site Request Forgery (CSRF) vulnerability in Store Locator plugin <= 1.4.5 on WordPress.<br>**CVE ID : CVE-2022-41615** | https://patchstack.com/database/vulnerability/agile-store-locator/wordpress-store-locator-plugin-1-4-5-cross-site- | A-AGI-STOR-121222/11 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | scripting-xss-via-cross-site-request-forgery-csrf-vulnerability?_s_id=cve, https://wordpress.org/plugins/agile-store-locator/ | |
| **Vendor: algolplus** | | | | | |
| **Product: phone_orders_for_woocommerce** | | | | | |
| Affected Version(s): * Up to (excluding) 3.7.2 | | | | | |
| N/A | 18-Nov-2022 | 6.5 | Auth. (subscriber+) Sensitive Data Exposure vulnerability in Phone Orders for WooCommerce plugin <= 3.7.1 on WordPress.<br>**CVE ID : CVE-2022-41655** | https://patchstack.com/database/vulnerability/phone-orders-for-woocommerce/wordpress-phone-orders-for-woocommerce-plugin-3-7-1-auth-sensitive-data-exposure-vulnerability?_s_id=cve, https://wordpress.org/plugins/phone-orders-for-woocommerce/#developers | A-ALG-PHON-121222/12 |
| **Vendor: aliyun-oss-client_project** | | | | | |
| **Product: aliyun-oss-client** | | | | | |
| Affected Version(s): * Up to (excluding) 0.8.1 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exposure of Sensitive Information to an Unauthorized Actor | 22-Nov-2022 | 4.3 | aliyun-oss-client is a rust client for Alibaba Cloud OSS. Users of this library will be affected, the incoming secret will be disclosed unintentionally. This issue has been patched in version 0.8.1.<br>**CVE ID : CVE-2022-39397** | https://github.com/tu6ge/oss-rs/commit/e4553f7d74fce682d802f8fb073943387796df29, https://github.com/tu6ge/oss-rs/security/advisories/GHSA-3w3h-7xgx-grwc | A-ALI-ALIY-121222/13 |
| **Vendor: amasty** | | | | | |
| **Product: blog_pro** | | | | | |
| Affected Version(s): * Up to (excluding) 2.10.5 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | The Preview functionality in the Amasty Blog Pro 2.10.3 plugin for Magento 2 uses eval unsafely. This allows attackers to perform Cross-site Scripting attacks on admin panel users by manipulating the generated preview application response.<br>**CVE ID : CVE-2022-36432** | N/A | A-AMA-BLOG-121222/14 |
| Affected Version(s): 2.10.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation | 23-Nov-2022 | 5.4 | Amasty Blog 2.10.3 is vulnerable to Cross Site Scripting (XSS) via leave comment functionality.<br>**CVE ID : CVE-2022-35500** | N/A | A-AMA-BLOG-121222/15 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | Stored Cross-site Scripting (XSS) exists in the Amasty Blog Pro 2.10.3 and 2.10.4 plugin for Magento 2 because of the duplicate post function.<br>**CVE ID : CVE-2022-35501** | N/A | A-AMA-BLOG-121222/16 |
| Affected Version(s): 2.10.4 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | Stored Cross-site Scripting (XSS) exists in the Amasty Blog Pro 2.10.3 and 2.10.4 plugin for Magento 2 because of the duplicate post function.<br>**CVE ID : CVE-2022-35501** | N/A | A-AMA-BLOG-121222/17 |
| **Vendor: Amazon** | | | | | |
| **Product: opensearch** | | | | | |
| Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.3.7 | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 16-Nov-2022 | 4.3 | OpenSearch is a community-driven, open source fork of Elasticsearch and Kibana. OpenSearch allows users to specify a local file when defining text analyzers to process data for text analysis. An issue in the implementation of this feature allows certain specially crafted queries to return a response | https://github.com/opensearch-project/OpenSearch/security/advisories/GHSA-w3rx-m34v-wrqx, https://github.com/opensearch-project/OpenSearch/commit/6d20423f5920745463b1 | A-AMA-OPEN-121222/18 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | containing the first line of text from arbitrary files. The list of potentially impacted files is limited to text files with read permissions allowed in the Java Security Manager policy configuration. OpenSearch version 1.3.7 and 2.4.0 contain a fix for this issue. Users are advised to upgrade. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-41917** | abc5f1daf6a786c41aa0 | |
| Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.4.0 | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 16-Nov-2022 | 4.3 | OpenSearch is a community-driven, open source fork of Elasticsearch and Kibana. OpenSearch allows users to specify a local file when defining text analyzers to process data for text analysis. An issue in the implementation of this feature allows certain specially crafted queries to return a response containing the first line of text from arbitrary files. The list of potentially impacted files is limited to text files with read permissions allowed in the Java | https://github.com/opensearch-project/OpenSearch/security/advisories/GHSA-w3rx-m34v-wrqx, https://github.com/opensearch-project/OpenSearch/commit/6d20423f5920745463b1abc5f1daf6a786c41aa0 | A-AMA-OPEN-121222/19 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Security Manager policy configuration. OpenSearch version 1.3.7 and 2.4.0 contain a fix for this issue. Users are advised to upgrade. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-41917** | | |
| **Vendor: analytics_for_wp_project** | | | | | |
| **Product: analytics_for_wp** | | | | | |
| Affected Version(s): * Up to (including) 1.5.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Analytics for WP WordPress plugin through 1.5.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3839** | N/A | A-ANA-ANAL-121222/20 |
| **Vendor: anthologize_project** | | | | | |
| **Product: anthologize** | | | | | |
| Affected Version(s): * Up to (excluding) 0.8.1 | | | | | |
| Improper Neutralization of Input During Web Page | 17-Nov-2022 | 4.8 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anthologize plugin <= 0.8.0 on WordPress. | https://patchstack.com/database/vulnerability/anthologize/wordpress- | A-ANT-ANTH-121222/21 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | **CVE ID : CVE-2022-44591** | anthologize-plugin-0-8-0-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve | |
| **Vendor: Apache** | | | | | |
| **Product: airflow** | | | | | |
| Affected Version(s): * Up to (excluding) 2.3.0 | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 9.8 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pig Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Pig Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Pig Provider is installed (Pig Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pig Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version. | https://github.com/apache/airflow/pull/27644 | A-APA-AIRF-121222/22 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-40189** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 7.8 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pinot Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Apache Airflow Pinot Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Apache Airflow Pinot Provider is installed (Apache Airflow Pinot Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pinot Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.<br>**CVE ID : CVE-2022-38649** | https://lists.apache.org/thread/033o1gbc4ly6dpd2xf1o201v56fbl4dz, https://github.com/apache/airflow/pull/27641 | A-APA-AIRF-121222/23 |
| Improper Neutralization of Special | 22-Nov-2022 | 7.8 | Improper Neutralization of Special Elements used in an OS Command | https://github.com/apache/airflow/pull/27647 | A-APA-AIRF-121222/24 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an OS Command ('OS Command Injection') | | | ('OS Command Injection') vulnerability in Apache Airflow Hive Provider, Apache Airflow allows an attacker to execute arbtrary commands in the task execution context, without write access to DAG files. This issue affects Hive Provider versions prior to 4.1.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case HIve Provider is installed (Hive Provider 4.1.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the HIve Provider version 4.1.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version that has lower version of the Hive Provider installed).<br>**CVE ID : CVE-2022-41131** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 22-Nov-2022 | 5.5 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Spark Provider, Apache Airflow allows an | https://lists.apache.org/thread/0tmdlnmjs5t4gsx5fy73tb6zd3jztq45,<br>https://github.com/apache/airflow/pull/27646 | A-APA-AIRF-121222/25 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | attacker to read arbtrary files in the task execution context, without write access to DAG files. This issue affects Spark Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Spark Provider is installed (Spark Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Spark Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version that has lower version of the Spark Provider installed).<br>**CVE ID : CVE-2022-40954** | | |
| **Product: alarm_instance_management** | | | | | |
| Affected Version(s): * Up to (excluding) 2.0.6 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | Alarm instance management has command injection when there is a specific command configured. It is only for logged-in users. We recommend you upgrade to version 2.0.6 or higher<br>**CVE ID : CVE-2022-45462** | https://lists.apache.org/thread/2f126y32bf1v3mvxkdgt2jr5j3l1t01w | A-APA-ALAR-121222/26 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: apache-airflow-providers-apache-hive** | | | | | |
| Affected Version(s): * Up to (excluding) 4.1.0 | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 7.8 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Hive Provider, Apache Airflow allows an attacker to execute arbtrary commands in the task execution context, without write access to DAG files. This issue affects Hive Provider versions prior to 4.1.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case HIve Provider is installed (Hive Provider 4.1.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the HIve Provider version 4.1.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version that has lower version of the Hive Provider installed).<br>**CVE ID : CVE-2022-41131** | https://github.com/apache/airflow/pull/27647 | A-APA-APAC-121222/27 |
| **Product: apache-airflow-providers-apache-pig** | | | | | |
| Affected Version(s): * Up to (excluding) 4.0.0 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 9.8 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pig Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Pig Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Pig Provider is installed (Pig Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pig Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.<br>**CVE ID : CVE-2022-40189** | https://github.com/apache/airflow/pull/27644 | A-APA-APAC-121222/28 |
| **Product: apache-airflow-providers-apache-pinot** | | | | | |
| Affected Version(s): * Up to (excluding) 4.0.0 | | | | | |
| Improper Neutralization of Special Elements used in an OS | 22-Nov-2022 | 7.8 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in | https://lists.apache.org/thread/033o1gbc4ly6dpd2xf1o201v56fbl4dz, https://githu | A-APA-APAC-121222/29 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('OS Command Injection') | | | Apache Airflow Pinot Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Apache Airflow Pinot Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Apache Airflow Pinot Provider is installed (Apache Airflow Pinot Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pinot Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.<br>**CVE ID : CVE-2022-38649** | b.com/apache/airflow/pull/27641 | |
| **Product: apache-airflow-providers-apache-spark** | | | | | |
| Affected Version(s): * Up to (excluding) 4.0.0 | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 22-Nov-2022 | 5.5 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Spark Provider, Apache Airflow allows an attacker to read | https://lists.apache.org/thread/0tmdlnmjs5t4gsx5fy73tb6zd3jztq45, https://github.com/apache/airflow/pull/27646 | A-APA-APAC-121222/30 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | arbtrary files in the task execution context, without write access to DAG files. This issue affects Spark Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Spark Provider is installed (Spark Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Spark Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version that has lower version of the Spark Provider installed).<br>**CVE ID : CVE-2022-40954** | | |
| **Product: hama** | | | | | |
| Affected Version(s): * Up to (including) 1.7.1 | | | | | |
| Improper Input Validation | 21-Nov-2022 | 7.5 | ** UNSUPPORTED WHEN ASSIGNED ** missing input validation in Apache Hama may cause information disclosure through path traversal and XSS. Since Apache Hama is EOL, we do not expect these issues to be fixed.<br>**CVE ID : CVE-2022-45470** | https://lists.apache.org/thread/ztvoshd4kxvp5vlro52mpgpfxct4ft8l | A-APA-HAMA-121222/31 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: sshd** | | | | | |
| Affected Version(s): * Up to (including) 2.9.1 | | | | | |
| Deserialization of Untrusted Data | 16-Nov-2022 | 9.8 | Class org.apache.sshd.server.keyprovider.SimpleGeneratorHostKeyProvider in Apache MINA SSHD <= 2.9.1 uses Java deserialization to load a serialized java.security.PrivateKey. The class is one of several implementations that an implementor using Apache MINA SSHD can choose for loading the host keys of an SSH server.<br>**CVE ID : CVE-2022-45047** | https://www.mail-archive.com/dev@mina.apache.org/msg39312.html | A-APA-SSHD-121222/32 |
| **Vendor: apartment_visitors_management_system_project** | | | | | |
| **Product: apartment_visitors_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 9.8 | Apartment Visitor Management System v1.0 is vulnerable to SQL Injection via /avms/index.php.<br>**CVE ID : CVE-2022-44139** | N/A | A-APA-APAR-121222/33 |
| **Vendor: api2cart** | | | | | |
| **Product: api2cart_bridge_connector** | | | | | |
| Affected Version(s): 1.0.0 | | | | | |
| Improper Neutralization of | 18-Nov-2022 | 9.8 | Arbitrary Code Execution vulnerability in | https://patchstack.com/database/vulner | A-API-API2-121222/34 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Special Elements used in an SQL Command ('SQL Injection') | | | Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.<br>**CVE ID : CVE-2022-42497** | ability/api2cart-bridge-connector/wordpress-api2cart-bridge-connector-plugin-1-1-0-arbitrary-code-execution-vulnerability?_s_id=cve, https://wordpress.org/plugins/api2cart-bridge-connector/#developers | |
| Unrestricted Upload of File with Dangerous Type | 18-Nov-2022 | 9.8 | Unauth. Arbitrary File Upload vulnerability in WordPress Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.<br>**CVE ID : CVE-2022-42698** | https://patchstack.com/database/vulnerability/api2cart-bridge-connector/wordpress-api2cart-bridge-connector-plugin-1-1-0-arbitrary-file-upload-vulnerability?_s_id=cve, https://wordpress.org/plugins/api2cart-bridge-connector/#developers | A-API-API2-121222/35 |
| Affected Version(s): 1.1.0 | | | | | |
| Improper Neutralizat | 18-Nov-2022 | 9.8 | Arbitrary Code Execution | https://patchstack.com/dat | A-API-API2-121222/36 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ion of Special Elements used in an SQL Command ('SQL Injection') | | | vulnerability in Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.<br>**CVE ID : CVE-2022-42497** | abase/vulnerability/api2cart-bridge-connector/wordpress-api2cart-bridge-connector-plugin-1-1-0-arbitrary-code-execution-vulnerability?_s_id=cve, https://wordpress.org/plugins/api2cart-bridge-connector/#developers | |
| Unrestricted Upload of File with Dangerous Type | 18-Nov-2022 | 9.8 | Unauth. Arbitrary File Upload vulnerability in WordPress Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.<br>**CVE ID : CVE-2022-42698** | https://patchstack.com/database/vulnerability/api2cart-bridge-connector/wordpress-api2cart-bridge-connector-plugin-1-1-0-arbitrary-file-upload-vulnerability?_s_id=cve, https://wordpress.org/plugins/api2cart-bridge-connector/#developers | A-API-API2-121222/37 |
| **Vendor: appsmith** | | | | | |
| **Product: appsmith** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (excluding) 1.8.2 | | | | | |
| Server-Side Request Forgery (SSRF) | 21-Nov-2022 | 6.5 | Server-Side Request Forgery (SSRF) in GitHub repository appsmithorg/appsmith prior to 1.8.2.<br>**CVE ID : CVE-2022-4096** | https://huntr.dev/bounties/7969e834-5982-456e-9683-861a7a5e2d22,<br>https://github.com/appsmithorg/appsmith/commit/769719ccfe667f059fe0b107a19ec9feb90f2e40 | A-APP-APPS-121222/38 |
| **Vendor: ARM** | | | | | |
| **Product: utgard_gpu_kernel_driver** | | | | | |
| Affected Version(s): r11p0 | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 23-Nov-2022 | 7.5 | An Arm product family through 2022-06-29 has a TOCTOU Race Condition that allows non-privileged user to make improper GPU processing operations to gain access to already freed memory.<br>**CVE ID : CVE-2022-34830** | https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities,<br>https://developer.arm.com/support/arm-security-updates | A-ARM-UTGA-121222/39 |
| Affected Version(s): r12p0 | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 23-Nov-2022 | 7.5 | An Arm product family through 2022-06-29 has a TOCTOU Race Condition that allows non-privileged user to make improper GPU processing operations | https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities,<br>https://devel | A-ARM-UTGA-121222/40 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to gain access to already freed memory.<br>**CVE ID : CVE-2022-34830** | oper.arm.com/support/arm-security-updates | |
| **Vendor: Artifex** | | | | | |
| **Product: mujs** | | | | | |
| Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.3.2 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 23-Nov-2022 | 8.8 | A logical issue in O_getOwnPropertyDescriptor() in Artifex MuJS 1.0.0 through 1.3.x before 1.3.2 allows an attacker to achieve Remote Code Execution through memory corruption, via the loading of a crafted JavaScript file.<br>**CVE ID : CVE-2022-44789** | https://github.com/alalng/CVE-2022-44789/blob/main/PublicReferenceURL.txt, https://github.com/ccxvii/mujs/commit/edb50ad66f7601ca9a3544a0e9045e8a8c60561f, https://github.com/ccxvii/mujs/releases/tag/1.3.2 | A-ART-MUJS-121222/41 |
| **Vendor: Atlassian** | | | | | |
| **Product: bitbucket** | | | | | |
| Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.6.19 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be | https://confluence.atlassian.com/x/Y4hXRg, https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/42 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | | |
| Affected Version(s): From (including) 7.18.0 Up to (excluding) 7.21.6 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | https://confluence.atlassian.com/x/Y4hXRg, https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/43 |
| Affected Version(s): From (including) 7.22.0 Up to (excluding) 8.0.5 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be | https://confluence.atlassian.com/x/Y4hXRg, https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/44 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | | |
| Affected Version(s): From (including) 7.7.0 Up to (excluding) 7.17.12 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | https://confluence.atlassian.com/x/Y4hXRg,<br>https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/45 |
| Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.5 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be | https://confluence.atlassian.com/x/Y4hXRg,<br>https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/46 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | | |
| Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.4 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | https://confluence.atlassian.com/x/Y4hXRg, https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/47 |
| Affected Version(s): From (including) 8.3.0 Up to (excluding) 8.3.3 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be | https://confluence.atlassian.com/x/Y4hXRg, https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/48 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | | |
| Affected Version(s): From (including) 8.4.0 Up to (excluding) 8.4.2 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | There is a command injection vulnerability using environment variables in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to execute arbitrary code on the system. This vulnerability can be unauthenticated if the Bitbucket Server and Data Center instance has enabled “Allow public signup”.<br>**CVE ID : CVE-2022-43781** | https://confluence.atlassian.com/x/Y4hXRg,<br>https://jira.atlassian.com/browse/BSERV-13522 | A-ATL-BITB-121222/49 |
| **Product: crowd** | | | | | |
| Affected Version(s): From (including) 3.0.0 Up to (excluding) 4.4.4 | | | | | |
| Improper Authentication | 17-Nov-2022 | 9.8 | Affected versions of Atlassian Crowd allow an attacker to authenticate as the crowd application via security misconfiguration and subsequent ability to call privileged endpoints in Crowd's REST API under the {{usermanagement}} | https://jira.atlassian.com/browse/CWD-5888 | A-ATL-CROW-121222/50 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | path. This vulnerability can only be exploited by IPs specified under the crowd application allowlist in the Remote Addresses configuration, which is {{none}} by default. The affected versions are all versions 3.x.x, versions 4.x.x before version 4.4.4, and versions 5.x.x before 5.0.3<br>**CVE ID : CVE-2022-43782** | | |
| Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.3 | | | | | |
| Improper Authentication | 17-Nov-2022 | 9.8 | Affected versions of Atlassian Crowd allow an attacker to authenticate as the crowd application via security misconfiguration and subsequent ability to call privileged endpoints in Crowd's REST API under the {{usermanagement}} path. This vulnerability can only be exploited by IPs specified under the crowd application allowlist in the Remote Addresses configuration, which is {{none}} by default. The affected versions are all versions 3.x.x, versions 4.x.x before version 4.4.4, and | https://jira.atlassian.com/browse/CWD-5888 | A-ATL-CROW-121222/51 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions 5.x.x before 5.0.3<br>**CVE ID : CVE-2022-43782** | | |
| **Vendor: audinate** | | | | | |
| **Product: dante_enabled_zoom_rooms** | | | | | |
| Affected Version(s): 1.3.0.0 | | | | | |
| Untrusted Search Path | 17-Nov-2022 | 7.8 | mDNSResponder.exe is vulnerable to DLL Sideloading attack. Executable improperly specifies how to load the DLL, from which folder and under what conditions. In these scenarios, a malicious attacker could be using the valid and legitimate executable to load malicious files.<br>**CVE ID : CVE-2022-23748** | N/A | A-AUD-DANT-121222/52 |
| **Vendor: Automattic** | | | | | |
| **Product: crowdsignal_dashboard** | | | | | |
| Affected Version(s): * Up to (excluding) 3.0.10 | | | | | |
| Improper Privilege Management | 17-Nov-2022 | 8.8 | Auth. (contributor+) Privilege Escalation vulnerability in Crowdsignal Dashboard plugin <= 3.0.9 on WordPress.<br>**CVE ID : CVE-2022-45069** | https://patchstack.com/database/vulnerability/polldaddy/wordpress-crowdsignal-dashboard-plugin-3-0-9-privilege-escalation-vulnerability?_s_id=cve | A-AUT-CROW-121222/53 |
| **Vendor: automotive_shop_management_system_project** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: automotive_shop_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL via /asms/classes/Master.php?f=delete_mechanic.<br>**CVE ID : CVE-2022-44378** | N/A | A-AUT-AUTO-121222/54 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/classes/Master.php?f=delete_service.<br>**CVE ID : CVE-2022-44379** | N/A | A-AUT-AUTO-121222/55 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/classes/Master.php?f=delete_transaction.<br>**CVE ID : CVE-2022-44402** | N/A | A-AUT-AUTO-121222/56 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/?page=user/manage_user&id=.<br>**CVE ID : CVE-2022-44403** | N/A | A-AUT-AUTO-121222/57 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/mechanics/manage_mechanic.php?id=.<br>**CVE ID : CVE-2022-44413** | N/A | A-AUT-AUTO-121222/58 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/services/manage_service.php?id=.<br>**CVE ID : CVE-2022-44414** | N/A | A-AUT-AUTO-121222/59 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/mechanics/view_mechanic.php?id=.<br>**CVE ID : CVE-2022-44415** | N/A | A-AUT-AUTO-121222/60 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 is vulnerable to SQL Injection via /asms/admin/?page=transactions/manage_transaction&id=.<br>**CVE ID : CVE-2022-44820** | N/A | A-AUT-AUTO-121222/61 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /asms/products/view_product.php.<br>**CVE ID : CVE-2022-44858** | N/A | A-AUT-AUTO-121222/62 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /asms/admin/products/manage_product.php.<br>**CVE ID : CVE-2022-44859** | N/A | A-AUT-AUTO-121222/63 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 7.2 | Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/transactions/update_status.php.<br>**CVE ID : CVE-2022-44860** | N/A | A-AUT-AUTO-121222/64 |
| Incorrect Permission Assignment for Critical Resource | 23-Nov-2022 | 6.5 | Automotive Shop Management System v1.0 is vulnerable to Delete any file via /asms/classes/Master.php?f=delete_img.<br>**CVE ID : CVE-2022-44280** | N/A | A-AUT-AUTO-121222/65 |
| **Vendor: awplife** | | | | | |
| **Product: event_monster** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (excluding) 1.2.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 21-Nov-2022 | 7.2 | The Event Monster WordPress plugin before 1.2.0 does not validate and escape some parameters before using them in SQL statements, which could lead to SQL Injection exploitable by high privilege users<br>**CVE ID : CVE-2022-3720** | https://wpscan.com/vulnerability/0139a23c-4896-4aef-ab56-dcf7f07f01e5 | A-AWP-EVEN-121222/66 |
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 4.3 | The Event Monster WordPress plugin before 1.2.0 does not have CSRF check when deleting visitors, which could allow attackers to make logged in admin delete arbitrary visitors via a CSRF attack<br>**CVE ID : CVE-2022-3336** | https://wpscan.com/vulnerability/57bc6633-1aeb-4c20-a2a5-9b3fa10ba95d | A-AWP-EVEN-121222/67 |
| **Vendor: backclick** | | | | | |
| **Product: backclick** | | | | | |
| Affected Version(s): 5.9.63 | | | | | |
| Missing Authentication for Critical Function | 16-Nov-2022 | 9.8 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to exposed CORBA management services, arbitrary system commands can be executed on the server.<br>**CVE ID : CVE-2022-43999** | N/A | A-BAC-BACK-121222/68 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authentication for Critical Function | 16-Nov-2022 | 9.8 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to an exposed internal communications interface, it is possible to execute arbitrary system commands on the server.<br>**CVE ID : CVE-2022-44000** | N/A | A-BAC-BACK-121222/69 |
| Missing Authentication for Critical Function | 17-Nov-2022 | 9.8 | An issue was discovered in BACKCLICK Professional 5.9.63. User authentication for accessing the CORBA back-end services can be bypassed.<br>**CVE ID : CVE-2022-44001** | N/A | A-BAC-BACK-121222/70 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Nov-2022 | 9.8 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to insufficient escaping of user-supplied input, the application is vulnerable to SQL injection at various locations.<br>**CVE ID : CVE-2022-44003** | N/A | A-BAC-BACK-121222/71 |
| Weak Password Recovery Mechanism for | 16-Nov-2022 | 9.8 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to insecure design | N/A | A-BAC-BACK-121222/72 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Forgotten Password | | | or lack of authentication, unauthenticated attackers can complete the password-reset process for any account and set a new password.<br>**CVE ID : CVE-2022-44004** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 16-Nov-2022 | 9.8 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to improper validation or sanitization of upload filenames, an externally reachable, unauthenticated update function permits writing files outside the intended target location. Achieving remote code execution is possible, e.g., by uploading an executable file.<br>**CVE ID : CVE-2022-44006** | N/A | A-BAC-BACK-121222/73 |
| Session Fixation | 16-Nov-2022 | 8.8 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to an unsafe implementation of session tracking, it is possible for an attacker to trick users into opening an authenticated user | N/A | A-BAC-BACK-121222/74 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | session for a session identifier known to the attacker, aka Session Fixation.<br>**CVE ID : CVE-2022-44007** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 16-Nov-2022 | 6.5 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to improper validation, arbitrary local files can be retrieved by accessing the back-end Tomcat server directly.<br>**CVE ID : CVE-2022-44008** | N/A | A-BAC-BACK-121222/75 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Nov-2022 | 6.1 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to insufficient output encoding of user-supplied data, the web application is vulnerable to cross-site scripting (XSS) at various locations.<br>**CVE ID : CVE-2022-44002** | N/A | A-BAC-BACK-121222/76 |
| Authorization Bypass Through User-Controlled Key | 16-Nov-2022 | 5.3 | An issue was discovered in BACKCLICK Professional 5.9.63. Due to the use of consecutive IDs in verification links, the newsletter sign-up functionality is vulnerable to the enumeration of | N/A | A-BAC-BACK-121222/77 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | subscribers' e-mail addresses. Furthermore, it is possible to subscribe and verify other persons' e-mail addresses to newsletters without their consent.<br>**CVE ID : CVE-2022-44005** | | |
| **Vendor: backdropcms** | | | | | |
| **Product: backdrop** | | | | | |
| Affected Version(s): 1.23.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 4.8 | Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the 'Card' content.<br>**CVE ID : CVE-2022-42094** | https://backdropcms.org | A-BAC-BACK-121222/78 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 4.8 | Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via 'Comment.' .<br>**CVE ID : CVE-2022-42097** | https://backdropcms.org | A-BAC-BACK-121222/79 |
| **Product: backdrop_cms** | | | | | |
| Affected Version(s): 1.23.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation | 21-Nov-2022 | 4.8 | Backdrop CMS version 1.23.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via Post content. | N/A | A-BAC-BACK-121222/80 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | **CVE ID : CVE-2022-42096** | | |
| **Vendor: beautiful-cookie-banner** | | | | | |
| **Product: beautiful_cookie_consent_banner** | | | | | |
| Affected Version(s): * Up to (excluding) 2.9.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Beautiful Cookie Consent Banner WordPress plugin before 2.9.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3823** | N/A | A-BEA-BEAU-121222/81 |
| **Vendor: beekeeperstudio** | | | | | |
| **Product: beekeeper-studio** | | | | | |
| Affected Version(s): 3.6.6 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 9.6 | A cross-site scripting (XSS) vulnerability in Beekeeper Studio v3.6.6 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the error modal container.<br>**CVE ID : CVE-2022-43143** | https://github.com/beekeeper-studio/beekeeper-studio/issues/1393 | A-BEE-BEEK-121222/82 |
| **Vendor: benbodhi** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: svg_support** | | | | | |
| Affected Version(s): From (including) 2.5.0 Up to (excluding) 2.5.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Nov-2022 | 5.4 | The SVG Support plugin for WordPress defaults to insecure settings in version 2.5 and 2.5.1. SVG files containing malicious javascript are not sanitized. While version 2.5 adds the ability to sanitize image as they are uploaded, the plugin defaults to disable sanitization and does not restrict SVG upload to only administrators. This allows authenticated attackers, with author-level privileges and higher, to upload malicious SVG files that can be embedded in posts and pages by higher privileged users. Additionally, the embedded JavaScript is also triggered on visiting the image URL, which allows an attacker to execute malicious code in browsers visiting that URL.<br>**CVE ID : CVE-2022-4022** | https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2776612%40svg-support%2Ftrunk&old=2672900%40svg-support%2Ftrunk&sfp_email=&sfph_mail= | A-BEN-SVG_-121222/83 |
| **Vendor: billing_system_project** | | | | | |
| **Product: billing_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 9.8 | Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the orderId parameter at printOrder.php.<br>**CVE ID : CVE-2022-43214** | N/A | A-BIL-BILL-121222/84 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 9.8 | Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the endDate parameter at getOrderReport.php.<br>**CVE ID : CVE-2022-43215** | N/A | A-BIL-BILL-121222/85 |
| **Vendor: billing_system_project_project** | | | | | |
| **Product: billing_system_project** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 9.8 | Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editorder.php.<br>**CVE ID : CVE-2022-43213** | N/A | A-BIL-BILL-121222/86 |
| **Vendor: billing_system_project_project_project** | | | | | |
| **Product: billing_system_project** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements | 22-Nov-2022 | 9.8 | Billing System Project v1.0 was discovered to contain a SQL injection vulnerability via the orderId | N/A | A-BIL-BILL-121222/87 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an SQL Command ('SQL Injection') | | | parameter at fetchOrderData.php.<br>**CVE ID : CVE-2022-43212** | | |
| **Vendor: blood_donor_management_system_project** | | | | | |
| **Product: blood_donor_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | Phpgurukul Blood Donor Management System 1.0 allows Cross Site Scripting via Add Blood Group Name Feature.<br>**CVE ID : CVE-2022-40470** | N/A | A-BLO-BLOO-121222/88 |
| **Vendor: BOA** | | | | | |
| **Product: boa** | | | | | |
| Affected Version(s): 0.94.14.21 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 9.8 | Boa 0.94.14rc21 is vulnerable to SQL Injection via username.<br>**CVE ID : CVE-2022-44117** | N/A | A-BOA-BOA-121222/89 |
| **Vendor: booster** | | | | | |
| **Product: booster_for_woocommerce** | | | | | |
| Affected Version(s): * Up to (excluding) 1.1.7 | | | | | |
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 8.1 | The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin | https://wpscan.com/vulnerability/7ab15530-8321-487d-97a5-1469b51fcc3f | A-BOO-BOOS-121222/90 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not have CSRF check in place when deleting files uploaded at the checkout, allowing attackers to make a logged in shop manager or admin delete them via a CSRF attack<br>**CVE ID : CVE-2022-3763** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 21-Nov-2022 | 6.5 | The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not validate files to download in some of its modules, which could allow ShopManager and Admin to download arbitrary files from the server even when they are not supposed to be able to (for example in multisite)<br>**CVE ID : CVE-2022-3762** | https://wpscan.com/vulnerability/96ef4bb8-a054-48ae-b29c-b3060acd01ac | A-BOO-BOOS-121222/91 |
| Affected Version(s): * Up to (excluding) 5.6.5 | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 8.1 | The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not have CSRF check in place when deleting files uploaded at the checkout, allowing attackers to make a logged in shop manager or admin delete them via a CSRF attack<br>**CVE ID : CVE-2022-3763** | https://wpscan.com/vulnerability/7ab15530-8321-487d-97a5-1469b51fcc3f | A-BOO-BOOS-121222/92 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 21-Nov-2022 | 6.5 | The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not validate files to download in some of its modules, which could allow ShopManager and Admin to download arbitrary files from the server even when | https://wpscan.com/vulnerability/96ef4bb8-a054-48ae-b29c-b3060acd01ac | A-BOO-BOOS-121222/93 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | they are not supposed to be able to (for example in multisite)<br>**CVE ID : CVE-2022-3762** | | |
| Affected Version(s): * Up to (excluding) 5.6.7 | | | | | |
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 8.1 | The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not have CSRF check in place when deleting files uploaded at the checkout, allowing attackers to make a logged in shop manager or admin delete them via a CSRF attack<br>**CVE ID : CVE-2022-3763** | https://wpscan.com/vulnerability/7ab15530-8321-487d-97a5-1469b51fcc3f | A-BOO-BOOS-121222/94 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 21-Nov-2022 | 6.5 | The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.5, Booster Elite for WooCommerce WordPress plugin before 1.1.7 do not validate files to | https://wpscan.com/vulnerability/96ef4bb8-a054-48ae-b29c-b3060acd01ac | A-BOO-BOOS-121222/95 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | download in some of its modules, which could allow ShopManager and Admin to download arbitrary files from the server even when they are not supposed to be able to (for example in multisite)<br>**CVE ID : CVE-2022-3762** |  |  |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 4.3 | Cross-Site Request Forgery (CSRF) vulnerability in Booster for WooCommerce plugin <= 5.6.6 on WordPress.<br>**CVE ID : CVE-2022-41805** | https://patchstack.com/database/vulnerability/woocommerce-jetpack/wordpress-booster-for-woocommerce-plugin-5-6-6-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | A-BOO-BOOS-121222/96 |
| **Vendor: btcd_project** |  |  |  |  |  |
| **Product: btcd** |  |  |  |  |  |
| Affected Version(s): * Up to (excluding) 0.23.3 |  |  |  |  |  |
| Improper Input Validation | 17-Nov-2022 | 6.5 | Lightning Network Daemon (lnd) is an implementation of a lightning bitcoin overlay network node. All lnd nodes before version `v0.15.4` are vulnerable to a block parsing bug that can cause a node to enter a degraded state once encountered. In this | https://github.com/lightningnetwork/lnd/issues/7096,<br>https://github.com/lightningnetwork/lnd/pull/7098,<br>https://github.com/lightningnetwork/ln | A-BTC-BTCD-121222/97 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | degraded state, nodes can continue to make payments and forward HTLCs, and close out channels. Opening channels is prohibited, and also on chain transaction events will be undetected. This can cause loss of funds if a CSV expiry is researched during a breach attempt or a CLTV delta expires forgetting the funds in the HTLC. A patch is available in `lnd` version 0.15.4. Users are advised to upgrade. Users unable to upgrade may use the `lncli updatechanpolicy` RPC call to increase their CLTV value to a very high amount or increase their fee policies. This will prevent nodes from routing through your node, meaning that no pending HTLCs can be present.<br>**CVE ID : CVE-2022-39389** | d/security/advisories/GHSA-hc82-w9v8-83pr |  |
| **Vendor: bund** |  |  |  |  |  |
| **Product: bkg_professional_ntripcaster** |  |  |  |  |  |
| Affected Version(s): * Up to (including) 2.0.39 |  |  |  |  |  |
| Missing Authentication for | 17-Nov-2022 | 7.5 | BKG Professional NtripCaster 2.0.39 allows querying information over the | https://igs.bkg.bund.de/ntrip/bkgcaster | A-BUN-BKG_-121222/98 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Critical Function | | | UDP protocol without authentication. The NTRIP sourcetable is typically quite long (tens of kBs) and can be requested with a packet of only 30 bytes. This presents a vector that can be used for UDP amplification attacks. Normally, only authenticated streaming data will be provided over UDP and not the sourcetable.<br>**CVE ID : CVE-2022-42982** | | |
| **Vendor: caehealthcare** | | | | | |
| **Product: learningspace_enterprise** | | | | | |
| Affected Version(s): image_267r | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | CAE LearningSpace Enterprise (with Intuity License) image 267r patch 639 allows DOM XSS, related to ontouchmove and onpointerup.<br>**CVE ID : CVE-2022-45472** | https://www.caehealthcare.com/learningspace/enterprise/ | A-CAE-LEAR-121222/99 |
| **Vendor: chameleon_project** | | | | | |
| **Product: chameleon** | | | | | |
| Affected Version(s): * Up to (excluding) 1.4.4 | | | | | |
| Improper Neutralization of Input During Web Page Generation | 17-Nov-2022 | 4.8 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Chameleon plugin <= 1.4.3 on WordPress. | https://patchstack.com/database/vulnerability/chameleon/wordpress-chameleon-plugin-1-4-3- | A-CHA-CHAM-121222/100 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | **CVE ID : CVE-2022-44736** | auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve | |
| **Vendor: churchcrm** | | | | | |
| **Product: churchcrm** | | | | | |
| Affected Version(s): 4.4.5 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 29-Nov-2022 | 4.8 | ChurchCRM Version 4.4.5 has XSS vulnerabilities that allow attackers to store XSS via location input Deposit Comment.<br>**CVE ID : CVE-2022-36136** | N/A | A-CHU-CHUR-121222/101 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 29-Nov-2022 | 4.8 | ChurchCRM Version 4.4.5 has XSS vulnerabilities that allow attackers to store XSS via location input sHeader.<br>**CVE ID : CVE-2022-36137** | N/A | A-CHU-CHUR-121222/102 |
| **Vendor: Ciphercoin** | | | | | |
| **Product: contact_form_7_database_addon** | | | | | |
| Affected Version(s): * Up to (excluding) 1.2.6.5 | | | | | |
| Improper Neutralization of Formula Elements in a CSV File | 21-Nov-2022 | 9.8 | The Contact Form 7 Database Addon WordPress plugin before 1.2.6.5 does not validate data when output it back in a CSV file, which could lead to CSV injection<br>**CVE ID : CVE-2022-3634** | https://wpscan.com/vulnerability/b5eeefb0-fb5e-4ca6-a6f0-67f4be4a2b10 | A-CIP-CONT-121222/103 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: clevelandwebdeveloper** | | | | | |
| **Product: spacer** | | | | | |
| Affected Version(s): * Up to (excluding) 3.0.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | The Spacer WordPress plugin before 3.0.7 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).<br>**CVE ID : CVE-2022-3618** | https://wpscan.com/vulnerability/2011dc7b-8e8c-4190-ab34-de288e14685b | A-CLE-SPAC-121222/104 |
| **Vendor: clogica** | | | | | |
| **Product: seo_redirection** | | | | | |
| Affected Version(s): * Up to (excluding) 9.1 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Multiple Cross-Site Scripting (CSRF) vulnerabilities in SEO Redirection Plugin plugin <= 8.9 on WordPress.<br>**CVE ID : CVE-2022-40695** | https://wordpress.org/plugins/seo-redirection/#developers, https://patchstack.com/database/vulnerability/seo-redirection/wordpress-seo-redirection-plugin-plugin-8-9-multiple-cross-site-scripting-csrf-vulnerabilities?_s_id=cve | A-CLO-SEO_-121222/105 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: cncf** | | | | | |
| **Product: knative_func** | | | | | |
| Affected Version(s): * Up to (excluding) 1.8.1 | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 19-Nov-2022 | 7.4 | knative.dev/func is is a client library and CLI enabling the development and deployment of Kubernetes functions. Developers using a malicious or compromised third-party buildpack could expose their registry credentials or local docker socket to a malicious `lifecycle` container. This issues has been patched in PR #1442, and is part of release 1.8.1. This issue only affects users who are using function buildpacks from third-parties; pinning the builder image to a specific content-hash with a valid `lifecycle` image will also mitigate the attack.<br>**CVE ID : CVE-2022-41939** | https://github.com/knative/func/pull/1442,<br>https://github.com/knative/func/security/advisories/GHSA-5336-2g3f-9g3m | A-CNC-KNAT-121222/106 |
| **Vendor: code-atlantic** | | | | | |
| **Product: popup_maker** | | | | | |
| Affected Version(s): * Up to (excluding) 1.16.11 | | | | | |
| Improper Neutralization of Input During | 21-Nov-2022 | 4.8 | The Popup Maker WordPress plugin before 1.16.11 does not sanitise and escape some of its | https://wpscan.com/vulnerability/725f6ae4-7ec5-4d7c-9533- | A-COD-POPU-121222/107 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | Popup options, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)<br>**CVE ID : CVE-2022-3690** | c9b61b59cc2b | |
| **Vendor: codenotary** | | | | | |
| **Product: immudb** | | | | | |
| Affected Version(s): * Up to (excluding) 1.4.1 | | | | | |
| Insufficient Verification of Data Authenticity | 22-Nov-2022 | 5.9 | immudb is a database with built-in cryptographic proof and verification. immudb client SDKs use server's UUID to distinguish between different server instance so that the client can connect to different immudb instances and keep the state for multiple servers. SDK does not validate this uuid and can accept any value reported by the server. A malicious server can change the reported UUID tricking the client to treat it as a different server thus accepting a state completely irrelevant to the one | https://github.com/codenotary/immudb/security/advisories/GHSA-6cqj-6969-p57x | A-COD-IMMU-121222/108 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | previously retrieved from the server. This issue has been patched in version 1.4.1. As a workaround, when initializing an immudb client object a custom state handler can be used to store the state. Providing custom implementation that ignores the server UUID can be used to ensure that even if the server changes the UUID, client will still consider it to be the same server.<br>**CVE ID : CVE-2022-39199** |  |  |
| Insufficient Verification of Data Authenticity | 23-Nov-2022 | 5.3 | immudb is a database with built-in cryptographic proof and verification. In versions prior to 1.4.1, a malicious immudb server can provide a falsified proof that will be accepted by the client SDK signing a falsified transaction replacing the genuine one. This situation can not be triggered by a genuine immudb server and requires the client to perform a specific list of verified operations resulting in acceptance of an invalid state value. This vulnerability only | https://github.com/codenotary/immudb/security/advisories/GHSA-672p-m5jq-mrh8 | A-COD-IMMU-121222/109 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | affects immudb client SDKs, the immudb server itself is not affected by this vulnerability. This issue has been patched in version 1.4.1.<br>**CVE ID : CVE-2022-36111** |  |  |
| **Vendor: Codepeople** |  |  |  |  |  |
| **Product: appointment_booking_calendar** |  |  |  |  |  |
| Affected Version(s): * Up to (excluding) 1.3.70 |  |  |  |  |  |
| Missing Authorization | 18-Nov-2022 | 8.8 | Missing Authorization vulnerability in Appointment Booking Calendar plugin <= 1.3.69 on WordPress.<br>**CVE ID : CVE-2022-43482** | https://patchstack.com/database/vulnerability/appointment-booking-calendar/wordpress-appointment-booking-calendar-plugin-1-3-69-missing-authorization-vulnerability?_s_id=cve | A-COD-APPO-121222/110 |
| **Vendor: college_management_system_project** |  |  |  |  |  |
| **Product: college_management_system** |  |  |  |  |  |
| Affected Version(s): 1.0 |  |  |  |  |  |
| Improper Neutralization of Special Elements used in an SQL Command | 17-Nov-2022 | 9.8 | College Management System v1.0 - SQL Injection (SQLi). By inserting SQL commands to the username and password fields in the login.php page. | N/A | A-COL-COLL-121222/111 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | **CVE ID : CVE-2022-39180** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 7.2 | College Management System v1.0 - Authenticated remote code execution. An admin user (the authentication can be bypassed using SQL Injection that mentioned in my other report) can upload .php file that contains malicious code via student.php file.<br>**CVE ID : CVE-2022-39179** | N/A | A-COL-COLL-121222/112 |
| **Vendor: collne** | | | | | |
| **Product: welcart_e-commerce** | | | | | |
| Affected Version(s): * Up to (excluding) 2.7.8 | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Nov-2022 | 9.8 | Unauth. Directory Traversal vulnerability in Welcart eCommerce plugin <= 2.7.7 on WordPress.<br>**CVE ID : CVE-2022-41840** | https://patchstack.com/database/vulnerability/usc-e-shop/wordpress-welcart-e-commerce-plugin-2-7-7-unauth-directory-traversal-vulnerability?_s_id=cve | A-COL-WELC-121222/113 |
| **Vendor: constantcontact** | | | | | |
| **Product: creative_mail** | | | | | |
| Affected Version(s): * Up to (excluding) 1.6.0 | | | | | |
| Cross-Site Request | 18-Nov-2022 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in | https://patchstack.com/database/vulner | A-CON-CREA-121222/114 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Forgery (CSRF) | | | Creative Mail plugin <= 1.5.4 on WordPress.<br>**CVE ID : CVE-2022-40686** | ability/creative-mail-by-constant-contact/wordpress-creative-mail-plugin-1-5-4-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Creative Mail plugin <= 1.5.4 on WordPress.<br>**CVE ID : CVE-2022-40687** | https://patchstack.com/database/vulnerability/creative-mail-by-constant-contact/wordpress-creative-mail-easier-wordpress-woocommerce-email-marketing-plugin-1-5-4-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | A-CON-CREA-121222/115 |
| Affected Version(s): * Up to (including) 1.5.4 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Creative Mail plugin <= 1.5.4 on WordPress.<br>**CVE ID : CVE-2022-44740** | https://wordpress.org/plugins/creative-mail-by-constant-contact/#developers | A-CON-CREA-121222/116 |
| **Vendor: cyberchimps** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: ifeature_slider** | | | | | |
| Affected Version(s): * Up to (including) 1.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Auth. Stored Cross-Site Scripting (XSS) vulnerability in iFeature Slider plugin <= 1.2 on WordPress.<br>**CVE ID : CVE-2022-45375** | https://patchstack.com/database/vulnerability/ifeature-slider/wordpress-ifeature-slider-plugin-1-2-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve | A-CYB-IFEA-121222/117 |
| **Vendor: dalli_project** | | | | | |
| **Product: dalli** | | | | | |
| Affected Version(s): From (including) - Up to (excluding) 3.2.3 | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 19-Nov-2022 | 3.7 | A vulnerability was found in Dalli. It has been classified as problematic. Affected is the function self.meta_set of the file lib/dalli/protocol/meta/request_formatter.rb of the component Meta Protocol Handler. The manipulation leads to injection. The exploit has been disclosed to the public and may be used. The name of the patch is 48d594dae55934476fec61789e7a7c3700e0f50d. It is recommended to apply a patch to fix this issue. VDB- | https://github.com/petergoldstein/dalli/commit/48d594dae55934476fec61789e7a7c3700e0f50d,<br>https://github.com/petergoldstein/dalli/pull/933 | A-DAL-DALL-121222/118 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 214026 is the identifier assigned to this vulnerability.<br>**CVE ID : CVE-2022-4064** | | |
| **Vendor: dedebiz** | | | | | |
| **Product: dedecmsv6** | | | | | |
| Affected Version(s): 6.1.9 | | | | | |
| N/A | 23-Nov-2022 | 9.8 | dedecmdv6 v6.1.9 is vulnerable to Remote Code Execution (RCE) via file_manage_control.php.<br>**CVE ID : CVE-2022-44118** | N/A | A-DED-DEDE-121222/119 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 9.8 | dedecmdv6 6.1.9 is vulnerable to SQL Injection. via sys_sql_query.php.<br>**CVE ID : CVE-2022-44120** | N/A | A-DED-DEDE-121222/120 |
| N/A | 23-Nov-2022 | 9.1 | dedecmdv6 v6.1.9 is vulnerable to Arbitrary file deletion via file_manage_control.php.<br>**CVE ID : CVE-2022-43196** | N/A | A-DED-DEDE-121222/121 |
| **Vendor: Dedecms** | | | | | |
| **Product: dedecms** | | | | | |
| Affected Version(s): 5.7.101 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unrestricted Upload of File with Dangerous Type | 17-Nov-2022 | 6.7 | An arbitrary file upload vulnerability in the component /dede/file_manage_control.php of Dedecms v5.7.101 allows attackers to execute arbitrary code via a crafted PHP file. This vulnerability is related to an incomplete fix for CVE-2022-40886.<br>**CVE ID : CVE-2022-43192** | N/A | A-DED-DEDE-121222/122 |
| **Vendor: deltaww** | | | | | |
| **Product: diaenergie** | | | | | |
| Affected Version(s): * Up to (excluding) 1.9.02.001 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 8.8 | SQL Injection in Handler_CFG.ashx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network<br>**CVE ID : CVE-2022-41775** | N/A | A-DEL-DIAE-121222/123 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 8.8 | SQL Injection in AM_EBillAnalysis.aspx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network<br>**CVE ID : CVE-2022-43447** | N/A | A-DEL-DIAE-121222/124 |
| Improper Neutralization of Special | 17-Nov-2022 | 8.8 | SQL Injection in FtyInfoSetting.aspx in Delta Electronics DIAEnergie versions | N/A | A-DEL-DIAE-121222/125 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an SQL Command ('SQL Injection') | | | prior to v1.9.02.001 allows an attacker to inject SQL queries via Network<br>**CVE ID : CVE-2022-43452** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 8.8 | SQL Injection in HandlerPage_KID.ashx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network<br>**CVE ID : CVE-2022-43457** | N/A | A-DEL-DIAE-121222/126 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 8.8 | SQL Injection in HandlerTag_KID.ashx in Delta Electronics DIAEnergie versions prior to v1.9.02.001 allows an attacker to inject SQL queries via Network<br>**CVE ID : CVE-2022-43506** | N/A | A-DEL-DIAE-121222/127 |
| **Vendor: Dolibarr** | | | | | |
| **Product: dolibarr_erp\/crm** | | | | | |
| Affected Version(s): * Up to (excluding) 14.0.1 | | | | | |
| Improper Privilege Management | 17-Nov-2022 | 9.8 | Dolibarr Open Source ERP & CRM for Business before v14.0.1 allows attackers to escalate privileges via a crafted API.<br>**CVE ID : CVE-2022-43138** | N/A | A-DOL-DOLI-121222/128 |
| Affected Version(s): 16.0.1 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 21-Nov-2022 | 9.8 | SQL injection attacks can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period. This affect 16.0.1 and 16.0.2 only. 16.0.0 or lower, and 16.0.3 or higher are not affected<br>**CVE ID : CVE-2022-4093** | https://github.com/dolibarr/dolibarr/commit/7c1eac9774bd1fed0b7b4594159f2ac2d12a4011, https://huntr.dev/bounties/677ca8ee-ffbc-4b39-b294-2ce81bd56788 | A-DOL-DOLI-121222/129 |
| Affected Version(s): 16.0.2 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 21-Nov-2022 | 9.8 | SQL injection attacks can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection | https://github.com/dolibarr/dolibarr/commit/7c1eac9774bd1fed0b7b4594159f2ac2d12a4011, https://huntr.dev/bounties/677ca8ee-ffbc-4b39- | A-DOL-DOLI-121222/130 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period. This affect 16.0.1 and 16.0.2 only. 16.0.0 or lower, and 16.0.3 or higher are not affected<br>**CVE ID : CVE-2022-4093** | b294-2ce81bd56788 | |
| **Vendor: drachtio** | | | | | |
| **Product: drachtio-server** | | | | | |
| Affected Version(s): 0.8.18 | | | | | |
| Use After Free | 18-Nov-2022 | 9.8 | drachtio-server 0.8.18 has a request-handler.cpp event_cb use-after-free for any request.<br>**CVE ID : CVE-2022-45474** | https://github.com/drachtio/drachtio-server/commit/860f025468feb31c43227153d8fb3f34210a522e | A-DRA-DRAC-121222/131 |
| N/A | 18-Nov-2022 | 5.5 | In drachtio-server 0.8.18, /var/log/drachtio has mode 0777 and drachtio.log has mode 0666.<br>**CVE ID : CVE-2022-45473** | https://github.com/drachtio/drachtio-server/commit/f791a9313c58a911ce09f465f4bba594243b29ec | A-DRA-DRAC-121222/132 |
| **Vendor: dreamer_cms_project** | | | | | |
| **Product: dreamer_cms** | | | | | |
| Affected Version(s): 4.0.01 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 9.8 | Dreamer CMS 4.0.01 is vulnerable to SQL Injection.<br>**CVE ID : CVE-2022-42245** | N/A | A-DRE-DREA-121222/133 |
| **Vendor: duofoxtechnologies** | | | | | |
| **Product: duofox_cms** | | | | | |
| Affected Version(s): 0.0.4 | | | | | |
| Cross-Site Request Forgery (CSRF) | 17-Nov-2022 | 8.8 | Doufox 0.0.4 contains a CSRF vulnerability that can add system administrator account.<br>**CVE ID : CVE-2022-42246** | N/A | A-DUO-DUOF-121222/134 |
| **Vendor: dwbooster** | | | | | |
| **Product: appointment_hour_booking** | | | | | |
| Affected Version(s): * Up to (excluding) 1.3.72 | | | | | |
| Missing Authorization | 18-Nov-2022 | 8.8 | Missing Authorization vulnerability in Appointment Hour Booking plugin <= 1.3.71 on WordPress.<br>**CVE ID : CVE-2022-41692** | https://patchstack.com/database/vulnerability/appointment-hour-booking/wordpress-appointment-hour-booking-plugin-1-3-71-missing-authorization-vulnerability?_s_id=cve | A-DWB-APPO-121222/135 |
| **Vendor: Emerson** | | | | | |
| **Product: proficy** | | | | | |
| Affected Version(s): * Up to (including) 9.00 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unrestricted Upload of File with Dangerous Type | 22-Nov-2022 | 7.8 | Emerson Electric's Proficy Machine Edition Version 9.00 and prior is vulnerable to CWE-434 Unrestricted Upload of File with Dangerous Type, and will upload any file written into the PLC logic folder to the connected PLC.<br>**CVE ID : CVE-2022-2791** | N/A | A-EME-PROF-121222/136 |
| **Vendor: equalweb** | | | | | |
| **Product: equalweb_accessibility_widget** | | | | | |
| Affected Version(s): 2.0.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/137 |
| Affected Version(s): 2.0.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js. | N/A | A-EQU-EQUA-121222/138 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-42960** | | |
| Affected Version(s): 2.0.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/139 |
| Affected Version(s): 2.0.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/140 |
| Affected Version(s): 2.0.4 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/141 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): 2.1.10 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/142 |
| Affected Version(s): 3.0.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/143 |
| Affected Version(s): 3.0.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/144 |
| Affected Version(s): 3.0.2 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/145 |
| Affected Version(s): 4.0.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/146 |
| Affected Version(s): 4.0.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | EqualWeb Accessibility Widget 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.1.10, 3.0.0, 3.0.1, 3.0.2, 4.0.0, and 4.0.1 allows DOM XSS due to improper validation of message events to accessibility.js.<br>**CVE ID : CVE-2022-42960** | N/A | A-EQU-EQUA-121222/147 |
| **Vendor: evaluate_project** | | | | | |
| **Product: evaluate** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (including) 1.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | The Evaluate WordPress plugin through 1.0 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).<br>**CVE ID : CVE-2022-3753** | https://wpscan.com/vulnerability/8e88a5b9-6f1d-40de-99fc-8e1e66646c2b | A-EVA-EVAL-121222/148 |
| **Vendor: event_registration_application_project** | | | | | |
| **Product: event_registration_application** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Formula Elements in a CSV File | 21-Nov-2022 | 7.8 | Sourcecodester Event Registration App v1.0 was discovered to contain multiple CSV injection vulnerabilities via the First Name, Contact and Remarks fields. These vulnerabilities allow attackers to execute arbitrary code via a crafted excel file.<br>**CVE ID : CVE-2022-44830** | N/A | A-EVE-EVEN-121222/149 |
| **Vendor: export_users_with_meta_project** | | | | | |
| **Product: export_users_with_meta** | | | | | |
| Affected Version(s): * Up to (including) 0.6.8 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Formula Elements in a CSV File | 17-Nov-2022 | 8 | This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.<br>**CVE ID : CVE-2022-44577** | https://wordpress.org/plugins/agenteasy-properties/, https://patchstack.com/database/vulnerability/agenteasy-properties/wordpress-agenteasy-properties-plugin-1-0-4-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve | A-EXP-EXPO-121222/150 |
| **Vendor: expresstech** | | | | | |
| **Product: quiz_and_survey_master** | | | | | |
| Affected Version(s): * Up to (excluding) 7.3.11 | | | | | |
| N/A | 18-Nov-2022 | 9.8 | Bypass vulnerability in Quiz And Survey Master plugin <= 7.3.10 on WordPress.<br>**CVE ID : CVE-2022-41652** | https://patchstack.com/database/vulnerability/quiz-master-next/wordpress-quiz-and-survey-master-plugin-7-3-10-bypass-vulnerability?_s_id=cve | A-EXP-QUIZ-121222/151 |
| Improper Neutralization of Input During Web Page Generation | 18-Nov-2022 | 6.1 | Auth. (subscriber+) Cross-Site Scripting (XSS) vulnerability in Quiz And Survey Master plugin <= 7.3.10 on WordPress. | https://patchstack.com/database/vulnerability/quiz-master-next/wordpress-quiz-and- | A-EXP-QUIZ-121222/152 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | **CVE ID : CVE-2022-40698** | survey-master-plugin-7-3-10-cross-site-scripting-xss-vulnerability?_s_id=cve | |
| Affected Version(s): * Up to (including) 7.3.10 | | | | | |
| N/A | 18-Nov-2022 | 7.5 | Sensitive Information Disclosure vulnerability discovered by Quiz And Survey Master plugin <= 7.3.10 on WordPress.<br>**CVE ID : CVE-2022-42883** | https://patchstack.com/database/vulnerability/quiz-master-next/wordpress-quiz-and-survey-master-plugin-7-3-10-sensitive-information-disclosure-vulnerability?_s_id=cve | A-EXP-QUIZ-121222/153 |
| **Vendor: eyoucms** | | | | | |
| **Product: eyoucms** | | | | | |
| Affected Version(s): 1.6.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | A cross-site scripting (XSS) vulnerability in the Url parameter in /login.php of EyouCMS v1.6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.<br>**CVE ID : CVE-2022-45280** | N/A | A-EYO-EYOU-121222/154 |
| **Vendor: eyunjing** | | | | | |
| **Product: yjcms** | | | | | |
| Affected Version(s): 1.0.9 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Insufficiently Protected Credentials | 23-Nov-2022 | 9.8 | An issue in the /index/user/user_edit.html component of YJCMS v1.0.9 allows unauthenticated attackers to obtain the Administrator account password.<br>**CVE ID : CVE-2022-45276** | N/A | A-EYU-YJCM-121222/155 |
| **Vendor: ezoic** | | | | | |
| **Product: ezoic** | | | | | |
| Affected Version(s): * Up to (including) 2.8.8 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 6.1 | Unauthenticated Plugin Settings Change Leading To Stored XSS Vulnerability in Ezoic plugin <= 2.8.8 on WordPress.<br>**CVE ID : CVE-2022-41132** | https://patchstack.com/database/vulnerability/ezoic-integration/wordpress-ezoic-plugin-2-8-8-unauthenticated-plugin-settings-change-leading-to-stored-xss-vulnerability?_s_id=cve | A-EZO-EZOI-121222/156 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 4.8 | Auth. Stored Cross-Site Scripting (XSS) vulnerability in Ezoic plugin <= 2.8.8 on WordPress.<br>**CVE ID : CVE-2022-41315** | https://patchstack.com/database/vulnerability/ezoic-integration/wordpress-ezoic-plugin-2-8-8-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve | A-EZO-EZOI-121222/157 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: fastify** | | | | | |
| **Product: fastify** | | | | | |
| Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.29.4 | | | | | |
| Cross-Site Request Forgery (CSRF) | 22-Nov-2022 | 8.8 | Fastify is a web framework with minimal overhead and plugin architecture. The attacker can use the incorrect `Content-Type` to bypass the `Pre-Flight` checking of `fetch`. `fetch()` requests with Content-Type's essence as "application/x-www-form-urlencoded", "multipart/form-data", or "text/plain", could potentially be used to invoke routes that only accepts `application/json` content type, thus bypassing any CORS protection, and therefore they could lead to a Cross-Site Request Forgery attack. This issue has been patched in version 4.10.2 and 3.29.4. As a workaround, implement Cross-Site Request Forgery protection using `@fastify/csrf'.<br>**CVE ID : CVE-2022-41919** | https://github.com/fastify/fastify/commit/62dde76f1f7aca76e38625fe8d983761f26e6fc9, https://github.com/fastify/fastify/security/advisories/GHSA-3fjj-p79j-c9hh | A-FAS-FAST-121222/158 |
| Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.10.2 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF) | 22-Nov-2022 | 8.8 | Fastify is a web framework with minimal overhead and plugin architecture. The attacker can use the incorrect `Content-Type` to bypass the `Pre-Flight` checking of `fetch`. `fetch()` requests with Content-Type's essence as "application/x-www-form-urlencoded", "multipart/form-data", or "text/plain", could potentially be used to invoke routes that only accepts `application/json` content type, thus bypassing any CORS protection, and therefore they could lead to a Cross-Site Request Forgery attack. This issue has been patched in version 4.10.2 and 3.29.4. As a workaround, implement Cross-Site Request Forgery protection using `@fastify/csrf'.<br>**CVE ID : CVE-2022-41919** | https://github.com/fastify/fastify/commit/62dde76f1f7aca76e38625fe8d983761f26e6fc9, https://github.com/fastify/fastify/security/advisories/GHSA-3fjj-p79j-c9hh | A-FAS-FAST-121222/159 |
| **Vendor: feehi** | | | | | |
| **Product: feehicms** | | | | | |
| Affected Version(s): - | | | | | |
| Cross-Site Request | 16-Nov-2022 | 4.3 | A vulnerability, which was classified as | N/A | A-FEE-FEEH-121222/160 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Forgery (CSRF) | | | problematic, has been found in FeehiCMS. Affected by this issue is some unknown functionality of the component Post My Comment Tab. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The identifier of this vulnerability is VDB-213788.<br>**CVE ID : CVE-2022-4014** | | |
| **Vendor: find_and_replace_all_project** | | | | | |
| **Product: find_and_replace_all** | | | | | |
| Affected Version(s): * Up to (excluding) 1.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 6.1 | The Find and Replace All WordPress plugin before 1.3 does not sanitize and escape some parameters from its setting page before outputting them back to the user, leading to a Reflected Cross-Site Scripting issue.<br>**CVE ID : CVE-2022-2311** | N/A | A-FIN-FIND-121222/161 |
| Affected Version(s): * Up to (including) 1.3 | | | | | |
| Cross-Site Request Forgery (CSRF) | 28-Nov-2022 | 4.3 | The Find and Replace All WordPress plugin before 1.3 does not have CSRF check when replacing string, which could allow attackers to make a | N/A | A-FIN-FIND-121222/162 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | logged admin replace arbitrary string in database tables via a CSRF attack<br>**CVE ID : CVE-2022-3850** | | |
| **Vendor: fivestarplugins** | | | | | |
| **Product: five_star_restaurant_reservations** | | | | | |
| Affected Version(s): * Up to (excluding) 2.4.12 | | | | | |
| Missing Authorization | 21-Nov-2022 | 6.1 | The Five Star Restaurant Reservations WordPress plugin before 2.4.12 does not have authorisation when changing whether a payment was successful or failed, allowing unauthenticated users to change the payment status of arbitrary bookings. Furthermore, due to the lack of sanitisation and escaping, attackers could perform Cross-Site Scripting attacks against a logged in admin viewing the failed payments<br>**CVE ID : CVE-2022-0421** | https://wpscan.com/vulnerability/145e8d3c-cd6f-4827-86e5-ea2d395a80b9 | A-FIV-FIVE-121222/163 |
| **Vendor: flarum** | | | | | |
| **Product: flarum** | | | | | |
| Affected Version(s): From (including) 1.5.0 Up to (excluding) 1.6.2 | | | | | |
| Improper Neutralization of Input | 19-Nov-2022 | 5.4 | Flarum is an open source discussion platform. Flarum's page title system | https://github.com/flarum/framework/security/advis | A-FLA-FLAR-121222/164 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | allowed for page titles to be converted into HTML DOM nodes when pages were rendered. The change was made after `v1.5` and was not noticed. This allowed an attacker to inject malicious HTML markup using a discussion title input, either by creating a new discussion or renaming one. The XSS attack occurs after a visitor opens the relevant discussion page. All communities running Flarum from `v1.5.0` to `v1.6.1` are impacted. The vulnerability has been fixed and published as flarum/core `v1.6.2`. All communities running Flarum from `v1.5.0` to `v1.6.1` have to upgrade as soon as possible to v1.6.2. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-41938** | ories/GHSA-7x4w-j98p-854x, https://github.com/flarum/framework/commit/690de9ce0ffe7ac4d45b73e303f44340c3433138, https://discuss.flarum.org/d/27558 | |
| **Vendor: fluenx** | | | | | |
| **Product: deepl_pro_api_translation** | | | | | |
| Affected Version(s): * Up to (excluding) 1.7.5 | | | | | |
| Insertion of Sensitive Informatio | 21-Nov-2022 | 7.5 | The DeepL Pro API translation plugin WordPress plugin before 1.7.5 discloses | https://wpscan.com/vulnerability/4248a0af-1b7e- | A-FLU-DEEP-121222/165 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n into Log File | | | sensitive information in its log files (which are publicly accessible), including DeepL API key.<br>**CVE ID : CVE-2022-3691** | 4e29-8129-3f40c1d0c560 | |
| **Vendor: Foxit** | | | | | |
| **Product: pdf_reader** | | | | | |
| Affected Version(s): 12.0.1.12430 | | | | | |
| Use After Free | 21-Nov-2022 | 7.8 | A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. By prematurely deleting objects associated with pages, a specially-crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.<br>**CVE ID : CVE-2022-32774** | N/A | A-FOX-PDF_-121222/166 |
| Use After Free | 21-Nov-2022 | 7.8 | A use-after-free vulnerability exists in the JavaScript engine | N/A | A-FOX-PDF_-121222/167 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of Foxit Software's PDF Reader, version 12.0.1.12430. A specially-crafted PDF document can trigger the reuse of previously freed memory via misusing media player API, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.<br>**CVE ID : CVE-2022-37332** | | |
| Use After Free | 21-Nov-2022 | 7.8 | A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. By prematurely destroying annotation objects, a specially-crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to | N/A | A-FOX-PDF_-121222/168 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.<br>**CVE ID : CVE-2022-38097** | | |
| Use After Free | 21-Nov-2022 | 7.8 | A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.0.1.12430. A specially-crafted PDF document can trigger the reuse of previously freed memory via misusing Optional Content Group API, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.<br>**CVE ID : CVE-2022-40129** | N/A | A-FOX-PDF_-121222/169 |
| **Vendor: free5gc** | | | | | |
| **Product: free5gc** | | | | | |
| Affected Version(s): 3.0.5 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncontrolled Resource Consumption | 18-Nov-2022 | 7.5 | In Free5gc v3.0.5, the AMF breaks due to malformed NAS messages.<br>**CVE ID : CVE-2022-38871** | N/A | A-FRE-FREE-121222/170 |
| **Vendor: Freedesktop** | | | | | |
| **Product: xdg-utils** | | | | | |
| Affected Version(s): From (including) 1.1.0 Up to (including) 1.1.3 | | | | | |
| Improper Neutralization of Expression/Command Delimiters | 19-Nov-2022 | 7.4 | When xdg-mail is configured to use thunderbird for mailto URLs, improper parsing of the URL can lead to additional headers being passed to thunderbird that should not be included per RFC 2368. An attacker can use this method to create a mailto URL that looks safe to users, but will actually attach files when clicked.<br>**CVE ID : CVE-2022-4055** | N/A | A-FRE-XDG--121222/171 |
| **Vendor: freerdp** | | | | | |
| **Product: freerdp** | | | | | |
| Affected Version(s): * Up to (excluding) 2.9.0 | | | | | |
| Out-of-bounds Read | 16-Nov-2022 | 5.7 | FreeRDP is a free remote desktop protocol library and clients. In affected versions there is an out of bound read in ZGFX decoder component of FreeRDP. A malicious server can trick a FreeRDP based client | https://github.com/FreeRDP/FreeRDP/commit/e865c24efc40ebc52e75979c94cdd4ee2c1495b0, https://github.com/FreeRDP/FreeRDP/ | A-FRE-FREE-121222/172 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to read out of bound data and try to decode it likely resulting in a crash. This issue has been addressed in the 2.9.0 release. Users are advised to upgrade.<br>**CVE ID : CVE-2022-39316** | security/advisories/GHSA-5w4j-mrrh-jjrm | |
| Divide By Zero | 16-Nov-2022 | 5.7 | FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing input validation in `urbdrc` channel. A malicious server can trick a FreeRDP based client to crash with division by zero. This issue has been addressed in version 2.9.0. All users are advised to upgrade. Users unable to upgrade should not use the `/usb` redirection switch.<br>**CVE ID : CVE-2022-39318** | https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-387j-8j96-7q35, https://github.com/FreeRDP/FreeRDP/commit/80adde17ddc4b596ed1dae0922a0c54ab3d4b8ea | A-FRE-FREE-121222/173 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 16-Nov-2022 | 5.7 | FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing path canonicalization and base path check for `drive` channel. A malicious server can trick a FreeRDP based client to read files | https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-c5xq-8v35-pffg, https://github.com/FreeRDP/FreeRDP/commit/027424c2c6c0991 | A-FRE-FREE-121222/174 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | outside the shared directory. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the `/drive`, `/drives` or `+home-drive` redirection switch.<br>**CVE ID : CVE-2022-39347** | cb9c22f9511478229c9b17e5d | |
| Out-of-bounds Read | 16-Nov-2022 | 4.6 | FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing a range check for input offset index in ZGFX decoder. A malicious server can trick a FreeRDP based client to read out of bound data and try to decode it. This issue has been addressed in version 2.9.0. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-39317** | https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-99cm-4gw7-c8jh | A-FRE-FREE-121222/175 |
| Out-of-bounds Read | 16-Nov-2022 | 4.6 | FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP are missing input length validation in the `urbdrc` channel. A malicious server can trick a FreeRDP based | https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-mvxm-wfj2-5fvh, https://github.com/FreeRDP/FreeRDP/ | A-FRE-FREE-121222/176 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | client to read out of bound data and send it back to the server. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the `/usb` redirection switch.<br>**CVE ID : CVE-2022-39319** | commit/11555828d2cf289b350baba5ad1f462f10b80b76 | |
| Out-of-bounds Read | 16-Nov-2022 | 4.6 | FreeRDP is a free remote desktop protocol library and clients. Affected versions of FreeRDP may attempt integer addition on too narrow types leads to allocation of a buffer too small holding the data written. A malicious server can trick a FreeRDP based client to read out of bound data and send it back to the server. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the `/usb` redirection switch.<br>**CVE ID : CVE-2022-39320** | https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-qfq2-82qr-7f4j | A-FRE-FREE-121222/177 |
| Out-of-bounds Read | 16-Nov-2022 | 4.6 | FreeRDP is a free remote desktop protocol library and clients. Affected | https://github.com/FreeRDP/FreeRDP/security/advi | A-FRE-FREE-121222/178 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions of FreeRDP are missing input length validation in `drive` channel. A malicious server can trick a FreeRDP based client to read out of bound data and send it back to the server. This issue has been addressed in version 2.9.0 and all users are advised to upgrade. Users unable to upgrade should not use the drive redirection channel - command line options `/drive`, `+drives` or `+home-drive`.<br>**CVE ID : CVE-2022-41877** | sories/GHSA-pmv3-wpw4-pw5h, https://github.com/FreeRDP/FreeRDP/commit/6655841cf2a00b764f855040aecb8803cfc5eaba | |
| **Vendor: fusiondirectory** | | | | | |
| **Product: fusiondirectory** | | | | | |
| Affected Version(s): 1.3 | | | | | |
| Insufficient Session Expiration | 22-Nov-2022 | 9.8 | Fusiondirectory 1.3 suffers from Improper Session Handling.<br>**CVE ID : CVE-2022-36179** | N/A | A-FUS-FUSI-121222/179 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 9.6 | Fusiondirectory 1.3 is vulnerable to Cross Site Scripting (XSS) via /fusiondirectory/index.php?message=[injection], /fusiondirectory/index.php?message=invalidparameter&plug={Injection], /fusiondirectory/index.php?signout=1&mes | N/A | A-FUS-FUSI-121222/180 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sage=[injection]&plug =106.<br>**CVE ID : CVE-2022-36180** | | |
| **Vendor: getawesomesupport** | | | | | |
| **Product: awesome_support** | | | | | |
| Affected Version(s): * Up to (excluding) 6.1.2 | | | | | |
| Authorization Bypass Through User-Controlled Key | 28-Nov-2022 | 6.5 | The Awesome Support WordPress plugin before 6.1.2 does not ensure that the exported tickets archive to be downloaded belongs to the user making the request, allowing a low privileged user, such as subscriber to download arbitrary exported tickets via an IDOR vector<br>**CVE ID : CVE-2022-3511** | N/A | A-GET-AWES-121222/181 |
| **Vendor: Glpi-project** | | | | | |
| **Product: reports** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 6.1 | GLPI - Reports plugin for GLPI Reflected Cross-Site-Scripting (RXSS). Type 1: Reflected XSS (or Non-Persistent) - The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply | N/A | A-GLP-REPO-121222/182 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.<br>**CVE ID : CVE-2022-39181** | | |
| **Vendor: Google** | | | | | |
| **Product: chrome** | | | | | |
| Affected Version(s): * Up to (excluding) 107.0.5304.121 | | | | | |
| Out-of-bounds Write | 25-Nov-2022 | 9.6 | Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to potentially perform a | https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_24.html | A-GOO-CHRO-121222/183 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sandbox escape via a crafted HTML page. (Chromium security severity: High)<br>**CVE ID : CVE-2022-4135** | | |
| **Product: tensorflow** | | | | | |
| Affected Version(s): * Up to (excluding) 2.7.4 | | | | | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.FusedResizeAndPadConv2D` is given a large tensor shape, it overflows. We have patched the issue in GitHub commit d66e1d568275e6a2947de97dca7a102a211e01ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41885** | https://github.com/tensorflow/tensorflow/commit/d66e1d568275e6a2947de97dca7a102a211e01ce, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-762h-vpvw-3rcx | A-GOO-TENS-121222/184 |
| Affected Version(s): * Up to (excluding) 2.8.4 | | | | | |
| Out-of-bounds Read | 18-Nov-2022 | 9.8 | TensorFlow is an open source platform for machine learning. The security vulnerability results in FractionalMax(AVG)Pool with illegal pooling_ratio. | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xvwp-h6jv-7472, https://githu | A-GOO-TENS-121222/185 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Attackers using Tensorflow can exploit the vulnerability. They can access heap memory which is not in the control of user, leading to a crash or remote code execution. We have patched the issue in GitHub commit 216525144ee7c910296f5b05d214ca1327c9ce48. The fix will be included in TensorFlow 2.11.0. We will also cherry pick this commit on TensorFlow 2.10.1.<br>**CVE ID : CVE-2022-41900** | b.com/tensorflow/tensorflow/commit/216525144ee7c910296f5b05d214ca1327c9ce48 | |
| Out-of-bounds Read | 18-Nov-2022 | 9.1 | TensorFlow is an open source platform for machine learning. When the `BaseCandidateSamplerOp` function receives a value in `true_classes` larger than `range_max`, a heap oob read occurs. We have patched the issue in GitHub commit b389f5c944cadfdfe599b3f1e4026e036f30d2d4. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8w5g-3wcv-9g2j, https://github.com/tensorflow/tensorflow/commit/b389f5c944cadfdfe599b3f1e4026e036f30d2d4 | A-GOO-TENS-121222/186 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41880** | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 18-Nov-2022 | 8.1 | TensorFlow is an open source platform for machine learning. The reference kernel of the `CONV_3D_TRANSPOSE` TensorFlow Lite operator wrongly increments the data_ptr when adding the bias to the result. Instead of `data_ptr += num_channels;` it should be `data_ptr += output_num_channels;` as if the number of input channels is different than the number of output channels, the wrong result will be returned and a buffer overflow will occur if num_channels > output_num_channels. An attacker can craft a model with a specific number of input channels. It is then possible to write specific values through the bias of the layer outside the bounds of the buffer. This attack only works if the reference kernel resolver is used in the interpreter. We have | https://github.com/tensorflow/tensorflow/commit/72c0bdcb25305b0b36842d746cc61d72658d2941, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h6q3-vv32-2cq5 | A-GOO-TENS-121222/187 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | patched the issue in GitHub commit 72c0bdcb25305b0b36842d746cc61d72658d2941. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41894** | | |
| Always-Incorrect Control Flow Implementation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If a numpy array is created with a shape such that one element is zero and the others sum to a large number, an error will be raised. We have patched the issue in GitHub commit 2b56169c16e375c521a3bc8ea658811cc0793784. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41884** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jq6x-99hj-q636, https://github.com/tensorflow/tensorflow/commit/2b56169c16e375c521a3bc8ea658811cc0793784 | A-GOO-TENS-121222/188 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ImageProjectiveTransformV2` is given a large output shape, it overflows. We have patched the issue in GitHub commit 8faa6ea692985dbe6ce10e1a3168e0bd60a723ba. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41886** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-54pp-c6pp-7fpx, https://github.com/tensorflow/tensorflow/commit/8faa6ea692985dbe6ce10e1a3168e0bd60a723ba | A-GOO-TENS-121222/189 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When running on GPU, `tf.image.generate_bounding_box_proposals` receives a `scores` input that must be of rank 4 but is not checked. We have patched the issue in GitHub commit cf35502463a88ca7185a99daa7031df60b3c1c98. The fix will be included in TensorFlow 2.11. We will also cherrypick | https://github.com/tensorflow/tensorflow/commit/cf35502463a88ca7185a99daa7031df60b3c1c98, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6x99-gv2v-q76v | A-GOO-TENS-121222/190 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41888** | | |
| NULL Pointer Dereference | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If a list of quantized tensors is assigned to an attribute, the pywrap code fails to parse the tensor and returns a `nullptr`, which is not caught. An example can be seen in `tf.compat.v1.extract_volume_patches` by passing in quantized tensors as input `ksizes`. We have patched the issue in GitHub commit e9e95553e5411834d215e6770c81a83a3d0866ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41889** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xxcj-rhqg-m46g, https://github.com/tensorflow/tensorflow/commit/e9e95553e5411834d215e6770c81a83a3d0866ce | A-GOO-TENS-121222/191 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Type Conversion or Cast | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `BCast::ToShape` is given input larger than an `int32`, it will crash, despite being supposed to handle up to an `int64`. An example can be seen in `tf.experimental.numpy.outer` by passing in large input to the input `b`. We have patched the issue in GitHub commit 8310bf8dd188ff780e7fc53245058215a05bdbe5. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41890** | https://github.com/tensorflow/tensorflow/commit/8310bf8dd188ff780e7fc53245058215a05bdbe5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h246-cgh4-7475 | A-GOO-TENS-121222/192 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListConcat` is given `element_shape=[]`, it results segmentation fault which can be used to trigger a denial of service attack. We have patched the issue in | https://github.com/tensorflow/tensorflow/commit/fc33f3dc4c14051a83eec6535b608abe1d355fde, https://github.com/tensorflow/tensorflow/security/a | A-GOO-TENS-121222/193 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | GitHub commit fc33f3dc4c14051a83eec6535b608abe1d355fde. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41891** | dvisories/GHSA-66vq-54fq-6jvv | |
| Reachable Assertion | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListResize` is given a nonscalar value for input `size`, it results `CHECK` fail which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 888e34b49009a4e734c27ab0c43b0b5102682c56. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41893** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-67pf-62xr-q35m, https://github.com/tensorflow/tensorflow/commit/888e34b49009a4e734c27ab0c43b0b5102682c56 | A-GOO-TENS-121222/194 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `MirrorPadGrad` is given outsize input `paddings`, TensorFlow will give a heap OOB error. We have patched the issue in GitHub commit 717ca98d8c3bba348ff62281fdf38dcb5ea1ec92. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41895** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gq2j-cr96-gvqx, https://github.com/tensorflow/tensorflow/commit/717ca98d8c3bba348ff62281fdf38dcb5ea1ec92 | A-GOO-TENS-121222/195 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `ThreadUnsafeUnigramCandidateSampler` is given input `filterbank_channel_count` greater than the allowed max size, TensorFlow will crash. We have patched the issue in GitHub commit 39ec7eaf1428e90c37787e5b3fbd68ebd3c48860. The fix will be included in TensorFlow 2.11. We will also cherrypick | https://github.com/tensorflow/tensorflow/commit/39ec7eaf1428e90c37787e5b3fbd68ebd3c48860, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rmg2-f698-wq35 | A-GOO-TENS-121222/196 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41896** | | |
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `FractionMaxPoolGrad` is given outsize inputs `row_pooling_sequence` and `col_pooling_sequence`, TensorFlow will crash. We have patched the issue in GitHub commit d71090c3e5ca325bdf4b02eb236cfb3ee823e927. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41897** | https://github.com/tensorflow/tensorflow/commit/d71090c3e5ca325bdf4b02eb236cfb3ee823e927, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f2w8-jw48-fr7j | A-GOO-TENS-121222/197 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `SparseFillEmptyRowsGrad` is given empty inputs, TensorFlow will crash. We have patched the issue in | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-hq7g-wwwp-q46h, https://githu | A-GOO-TENS-121222/198 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | GitHub commit af4a6a3c8b95022c351edae94560acc61253a1b8. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41898** | b.com/tensorflow/tensorflow/commit/af4a6a3c8b95022c351edae94560acc61253a1b8 | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. Inputs `dense_features` or `example_state_data` not of rank 2 will trigger a `CHECK` fail in `SdcaOptimizer`. We have patched the issue in GitHub commit 80ff197d03db2a70c6a111f97dcdacad1b0babfa. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41899** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-27rc-728f-x5w2,<br>https://github.com/tensorflow/tensorflow/commit/80ff197d03db2a70c6a111f97dcdacad1b0babfa | A-GOO-TENS-121222/199 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `sparse_matrix` that is not a matrix with a shape with rank 0 will trigger a `CHECK` fail in `tf.raw_ops.SparseMatrixNNZ`. We have patched the issue in GitHub commit f856d02e5322821aad155dad9b3acab1e9f5d693. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41901** | https://github.com/tensorflow/tensorflow/commit/f856d02e5322821aad155dad9b3acab1e9f5d693, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9fm-r5mm-rf9f | A-GOO-TENS-121222/200 |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ResizeNearestNeighborGrad` is given a large `size` input, it overflows. We have patched the issue in GitHub commit 00c821af032ba9e5f5fa3fe14690c8d28a657624. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on | https://github.com/tensorflow/tensorflow/commit/00c821af032ba9e5f5fa3fe14690c8d28a657624, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-368v-7v32-52fx | A-GOO-TENS-121222/201 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41907** | | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `token` that is not a UTF-8 bytestring will trigger a `CHECK` fail in `tf.raw_ops.PyFunc`. We have patched the issue in GitHub commit 9f03a9d3bafe902c1e6beb105b2f24172f238645. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41908** | https://github.com/tensorflow/tensorflow/commit/9f03a9d3bafe902c1e6beb105b2f24172f238645, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv77-9g28-cwg3 | A-GOO-TENS-121222/202 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `encoded` that is not a valid `CompositeTensorVariant` tensor will trigger a segfault in `tf.raw_ops.CompositeTensorVariantToComponents`. We have | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rjx6-v474-2ch9, https://github.com/tensorflow/tensorflow/commit/66 | A-GOO-TENS-121222/203 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | patched the issue in GitHub commits bf594d08d377dc6a3354d9fdb494b32d45f91971 and 660ce5a89eb6766834bdc303d2ab3902aef99d3d. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41909** | 0ce5a89eb6766834bdc303d2ab3902aef99d3d | |
| Incorrect Type Conversion or Cast | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When printing a tensor, we get it's data as a `const char*` array (since that's the underlying storage) and then we typecast it to the element type. However, conversions from `char` to `bool` are undefined if the `char` is not `0` or `1`, so sanitizers/fuzzers will crash. The issue has been patched in GitHub commit `1be74370327`. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on | https://github.com/tensorflow/tensorflow/commit/1be743703279782a357adbf9b77dcb994fe8b508, https://github.com/tensorflow/tensorflow/blob/807cae8a807960fd7ac2313cde73a11fc15e7942/tensorflow/core/framework/tensor.cc#L1200-L1227 | A-GOO-TENS-121222/204 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | TensorFlow 2.10.1, TensorFlow 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41911** |  |  |
| Affected Version(s): 2.10 |  |  |  |  |  |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. Inputs `dense_features` or `example_state_data` not of rank 2 will trigger a `CHECK` fail in `SdcaOptimizer`. We have patched the issue in GitHub commit 80ff197d03db2a70c6a111f97dcdacad1b0babfa. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41899** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-27rc-728f-x5w2, https://github.com/tensorflow/tensorflow/commit/80ff197d03db2a70c6a111f97dcdacad1b0babfa | A-GOO-TENS-121222/205 |
| Affected Version(s): 2.10.0 |  |  |  |  |  |
| Out-of-bounds Read | 18-Nov-2022 | 9.8 | TensorFlow is an open source platform for machine learning. The security vulnerability results in FractionalMax(AVG)Pool with illegal | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xvwp-h6jv-7472, | A-GOO-TENS-121222/206 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pooling_ratio. Attackers using Tensorflow can exploit the vulnerability. They can access heap memory which is not in the control of user, leading to a crash or remote code execution. We have patched the issue in GitHub commit 216525144ee7c910296f5b05d214ca1327c9ce48. The fix will be included in TensorFlow 2.11.0. We will also cherry pick this commit on TensorFlow 2.10.1.<br>**CVE ID : CVE-2022-41900** | https://github.com/tensorflow/tensorflow/commit/216525144ee7c910296f5b05d214ca1327c9ce48 | |
| Out-of-bounds Read | 18-Nov-2022 | 9.1 | TensorFlow is an open source platform for machine learning. When the `BaseCandidateSamplerOp` function receives a value in `true_classes` larger than `range_max`, a heap oob read occurs. We have patched the issue in GitHub commit b389f5c944cadfdfe599b3f1e4026e036f30d2d4. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8w5g-3wcv-9g2j, https://github.com/tensorflow/tensorflow/commit/b389f5c944cadfdfe599b3f1e4026e036f30d2d4 | A-GOO-TENS-121222/207 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41880** | | |
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When ops that have specified input sizes receive a differing number of inputs, the executor will crash. We have patched the issue in GitHub commit f5381e0e10b5a61344109c1b7c174c68110f7629. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41883** | https://github.com/tensorflow/tensorflow/commit/f5381e0e10b5a61344109c1b7c174c68110f7629, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-w58w-79xv-6vcj | A-GOO-TENS-121222/208 |
| Always-Incorrect Control Flow Implementation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If a numpy array is created with a shape such that one element is zero and the others sum to a large number, an error will be raised. We have patched the issue in | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jq6x-99hj-q636, https://github.com/tensorflow/tensorflow/commit/2b | A-GOO-TENS-121222/209 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | GitHub commit 2b56169c16e375c521a3bc8ea658811cc0793784. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41884** | 56169c16e375c521a3bc8ea658811cc0793784 | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.FusedResizeAndPadConv2D` is given a large tensor shape, it overflows. We have patched the issue in GitHub commit d66e1d568275e6a2947de97dca7a102a211e01ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41885** | https://github.com/tensorflow/tensorflow/commit/d66e1d568275e6a2947de97dca7a102a211e01ce, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-762h-vpvw-3rcx | A-GOO-TENS-121222/210 |
| Incorrect Calculation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. | https://github.com/tensorflo | A-GOO-TENS-121222/211 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Buffer Size | | | When `tf.raw_ops.ImageProjectiveTransformV2` is given a large output shape, it overflows. We have patched the issue in GitHub commit 8faa6ea692985dbe6ce10e1a3168e0bd60a723ba. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41886** | w/security/advisories/GHSA-54pp-c6pp-7fpx, https://github.com/tensorflow/tensorflow/commit/8faa6ea692985dbe6ce10e1a3168e0bd60a723ba | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. `tf.keras.losses.poisson` receives a `y_pred` and `y_true` that are passed through `functor::mul` in `BinaryOp`. If the resulting dimensions overflow an `int32`, TensorFlow will crash due to a size mismatch during broadcast assignment. We have patched the issue in GitHub commit c5b30379ba87cbe774b08ac50c1f6d36df4ebb7c. The fix will be included in | https://github.com/tensorflow/tensorflow/commit/c5b30379ba87cbe774b08ac50c1f6d36df4ebb7c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8fvv-46hw-vpg3 | A-GOO-TENS-121222/212 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1 and 2.9.3, as these are also affected and still in supported range. However, we will not cherrypick this commit into TensorFlow 2.8.x, as it depends on Eigen behavior that changed between 2.8 and 2.9.<br>**CVE ID : CVE-2022-41887** | | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `token` that is not a UTF-8 bytestring will trigger a `CHECK` fail in `tf.raw_ops.PyFunc`. We have patched the issue in GitHub commit 9f03a9d3bafe902c1e6beb105b2f24172f238645. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41908** | https://github.com/tensorflow/tensorflow/commit/9f03a9d3bafe902c1e6beb105b2f24172f238645, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv77-9g28-cwg3 | A-GOO-TENS-121222/213 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `encoded` that is not a valid `CompositeTensorVariant` tensor will trigger a segfault in `tf.raw_ops.CompositeTensorVariantToComponents`. We have patched the issue in GitHub commits bf594d08d377dc6a3354d9fdb494b32d45f91971 and 660ce5a89eb6766834bdc303d2ab3902aef99d3d. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41909** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rjx6-v474-2ch9, https://github.com/tensorflow/tensorflow/commit/660ce5a89eb6766834bdc303d2ab3902aef99d3d | A-GOO-TENS-121222/214 |
| Incorrect Type Conversion or Cast | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When printing a tensor, we get it's data as a `const char*` array (since that's the underlying storage) and then we typecast it to the element type. However, conversions from `char` to `bool` are undefined if the | https://github.com/tensorflow/tensorflow/commit/1be743703279782a357adbf9b77dcb994fe8b508, https://github.com/tensorflow/tensorflow/blob/807cae8a807960f | A-GOO-TENS-121222/215 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | `char` is not `0` or `1`, so sanitizers/fuzzers will crash. The issue has been patched in GitHub commit `1be74370327`. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.10.1, TensorFlow 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41911** | d7ac2313cde73a11fc15e7942/tensorflow/core/framework/tensor.cc#L1200-L1227 | |
| Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.1 | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 18-Nov-2022 | 8.1 | TensorFlow is an open source platform for machine learning. The reference kernel of the `CONV_3D_TRANSPOSE` TensorFlow Lite operator wrongly increments the data_ptr when adding the bias to the result. Instead of `data_ptr += num_channels;` it should be `data_ptr += output_num_channels;` as if the number of input channels is different than the number of output channels, the wrong result will be returned and a buffer overflow will occur if num_channels > | https://github.com/tensorflow/tensorflow/commit/72c0bdcb25305b0b36842d746cc61d72658d2941, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h6q3-vv32-2cq5 | A-GOO-TENS-121222/216 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | output_num_channels. An attacker can craft a model with a specific number of input channels. It is then possible to write specific values through the bias of the layer outside the bounds of the buffer. This attack only works if the reference kernel resolver is used in the interpreter. We have patched the issue in GitHub commit 72c0bdcb25305b0b36842d746cc61d72658d2941. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41894** |  |  |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When running on GPU, `tf.image.generate_bounding_box_proposals` receives a `scores` input that must be of rank 4 but is not checked. We have patched the issue in GitHub commit cf35502463a88ca718 | https://github.com/tensorflow/tensorflow/commit/cf35502463a88ca7185a99daa7031df60b3c1c98, https://github.com/tensorflow/tensorflow/security/advisories/GH | A-GOO-TENS-121222/217 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 5a99daa7031df60b3c1c98. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41888** | SA-6x99-gv2v-q76v | |
| NULL Pointer Dereference | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If a list of quantized tensors is assigned to an attribute, the pywrap code fails to parse the tensor and returns a `nullptr`, which is not caught. An example can be seen in `tf.compat.v1.extract_volume_patches` by passing in quantized tensors as input `ksizes`. We have patched the issue in GitHub commit e9e95553e5411834d215e6770c81a83a3d0866ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xxcj-rhqg-m46g, https://github.com/tensorflow/tensorflow/commit/e9e95553e5411834d215e6770c81a83a3d0866ce | A-GOO-TENS-121222/218 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected and still in supported range.<br>**CVE ID : CVE-2022-41889** | | |
| Incorrect Type Conversion or Cast | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `BCast::ToShape` is given input larger than an `int32`, it will crash, despite being supposed to handle up to an `int64`. An example can be seen in `tf.experimental.numpy.outer` by passing in large input to the input `b`. We have patched the issue in GitHub commit 8310bf8dd188ff780e7fc53245058215a05bdbe5. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41890** | https://github.com/tensorflow/tensorflow/commit/8310bf8dd188ff780e7fc53245058215a05bdbe5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h246-cgh4-7475 | A-GOO-TENS-121222/219 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListConcat` is given `element_shape=[]`, it results segmentation fault which can be | https://github.com/tensorflow/tensorflow/commit/fc33f3dc4c14051a83eec6535b608abe1d355fde, | A-GOO-TENS-121222/220 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | used to trigger a denial of service attack. We have patched the issue in GitHub commit fc33f3dc4c14051a83eec6535b608abe1d355fde. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41891** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-66vq-54fq-6jvv | |
| Reachable Assertion | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListResize` is given a nonscalar value for input `size`, it results `CHECK` fail which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 888e34b49009a4e734c27ab0c43b0b5102682c56. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-67pf-62xr-q35m, https://github.com/tensorflow/tensorflow/commit/888e34b49009a4e734c27ab0c43b0b5102682c56 | A-GOO-TENS-121222/221 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected and still in supported range.<br>**CVE ID : CVE-2022-41893** | | |
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `MirrorPadGrad` is given outsize input `paddings`, TensorFlow will give a heap OOB error. We have patched the issue in GitHub commit 717ca98d8c3bba348ff62281fdf38dcb5ea1ec92. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41895** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gq2j-cr96-gvqx, https://github.com/tensorflow/tensorflow/commit/717ca98d8c3bba348ff62281fdf38dcb5ea1ec92 | A-GOO-TENS-121222/222 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `ThreadUnsafeUnigramCandidateSampler` is given input `filterbank_channel_count` greater than the allowed max size, TensorFlow will crash. We have patched the issue in GitHub commit 39ec7eaf1428e90c37787e5b3fbd68ebd3c4 | https://github.com/tensorflow/tensorflow/commit/39ec7eaf1428e90c37787e5b3fbd68ebd3c48860, https://github.com/tensorflow/tensorflow/security/advisories/GH | A-GOO-TENS-121222/223 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 8860. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41896** | SA-rmg2-f698-wq35 | |
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `FractionMaxPoolGrad` is given outsize inputs `row_pooling_sequence` and `col_pooling_sequence`, TensorFlow will crash. We have patched the issue in GitHub commit d71090c3e5ca325bdf4b02eb236cfb3ee823e927. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41897** | https://github.com/tensorflow/tensorflow/commit/d71090c3e5ca325bdf4b02eb236cfb3ee823e927, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f2w8-jw48-fr7j | A-GOO-TENS-121222/224 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `SparseFillEmptyRows | https://github.com/tensorflow/tensorflow/security/a | A-GOO-TENS-121222/225 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Grad` is given empty inputs, TensorFlow will crash. We have patched the issue in GitHub commit af4a6a3c8b95022c351edae94560acc61253a1b8. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41898** | dvisories/GHSA-hq7g-wwwp-q46h, https://github.com/tensorflow/tensorflow/commit/af4a6a3c8b95022c351edae94560acc61253a1b8 | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `sparse_matrix` that is not a matrix with a shape with rank 0 will trigger a `CHECK` fail in `tf.raw_ops.SparseMatrixNNZ`. We have patched the issue in GitHub commit f856d02e5322821aad155dad9b3acab1e9f5d693. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range. | https://github.com/tensorflow/tensorflow/commit/f856d02e5322821aad155dad9b3acab1e9f5d693, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9fm-r5mm-rf9f | A-GOO-TENS-121222/226 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-41901** | | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ResizeNearestNeighborGrad` is given a large `size` input, it overflows. We have patched the issue in GitHub commit 00c821af032ba9e5f5fa3fe14690c8d28a657624. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41907** | https://github.com/tensorflow/tensorflow/commit/00c821af032ba9e5f5fa3fe14690c8d28a657624,<br>https://github.com/tensorflow/tensorflow/security/advisories/GHSA-368v-7v32-52fx | A-GOO-TENS-121222/227 |
| Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.1 | | | | | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.FusedResizeAndPadConv2D` is given a large tensor shape, it overflows. We have patched the issue in GitHub commit d66e1d568275e6a2947de97dca7a102a211e01ce. The fix will be included in TensorFlow 2.11. We | https://github.com/tensorflow/tensorflow/commit/d66e1d568275e6a2947de97dca7a102a211e01ce,<br>https://github.com/tensorflow/tensorflow/security/advisories/GHSA-762h-vpvw-3rcx | A-GOO-TENS-121222/228 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41885** |  |  |
| Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.1 |  |  |  |  |  |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.FusedResizeAndPadConv2D` is given a large tensor shape, it overflows. We have patched the issue in GitHub commit d66e1d568275e6a2947de97dca7a102a211e01ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41885** | https://github.com/tensorflow/tensorflow/commit/d66e1d568275e6a2947de97dca7a102a211e01ce, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-762h-vpvw-3rcx | A-GOO-TENS-121222/229 |
| Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.3 |  |  |  |  |  |
| Out-of-bounds Read | 18-Nov-2022 | 9.8 | TensorFlow is an open source platform for machine learning. The security vulnerability results in FractionalMax(AVG)P | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xvwp- | A-GOO-TENS-121222/230 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ool with illegal pooling_ratio. Attackers using Tensorflow can exploit the vulnerability. They can access heap memory which is not in the control of user, leading to a crash or remote code execution. We have patched the issue in GitHub commit 216525144ee7c910296f5b05d214ca1327c9ce48. The fix will be included in TensorFlow 2.11.0. We will also cherry pick this commit on TensorFlow 2.10.1.<br>**CVE ID : CVE-2022-41900** | h6jv-7472, https://github.com/tensorflow/tensorflow/commit/216525144ee7c910296f5b05d214ca1327c9ce48 | |
| Out-of-bounds Read | 18-Nov-2022 | 9.1 | TensorFlow is an open source platform for machine learning. When the `BaseCandidateSamplerOp` function receives a value in `true_classes` larger than `range_max`, a heap oob read occurs. We have patched the issue in GitHub commit b389f5c944cadfdfe599b3f1e4026e036f30d2d4. The fix will be included in TensorFlow 2.11. We will also cherrypick | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8w5g-3wcv-9g2j, https://github.com/tensorflow/tensorflow/commit/b389f5c944cadfdfe599b3f1e4026e036f30d2d4 | A-GOO-TENS-121222/231 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41880** |  |  |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 18-Nov-2022 | 8.1 | TensorFlow is an open source platform for machine learning. The reference kernel of the `CONV_3D_TRANSPOSE` TensorFlow Lite operator wrongly increments the data_ptr when adding the bias to the result. Instead of `data_ptr += num_channels;` it should be `data_ptr += output_num_channels;` as if the number of input channels is different than the number of output channels, the wrong result will be returned and a buffer overflow will occur if num_channels > output_num_channels. An attacker can craft a model with a specific number of input channels. It is then possible to write specific values through the bias of the layer outside the bounds of the buffer. This attack only works if the reference kernel | https://github.com/tensorflow/tensorflow/commit/72c0bdcb25305b0b36842d746cc61d72658d2941, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h6q3-vv32-2cq5 | A-GOO-TENS-121222/232 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | resolver is used in the interpreter. We have patched the issue in GitHub commit 72c0bdcb25305b0b36842d746cc61d72658d2941. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41894** |  |  |
| Always-Incorrect Control Flow Implementation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If a numpy array is created with a shape such that one element is zero and the others sum to a large number, an error will be raised. We have patched the issue in GitHub commit 2b56169c16e375c521a3bc8ea658811cc0793784. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range. | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jq6x-99hj-q636, https://github.com/tensorflow/tensorflow/commit/2b56169c16e375c521a3bc8ea658811cc0793784 | A-GOO-TENS-121222/233 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-41884** | | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ImageProjectiveTransformV2` is given a large output shape, it overflows. We have patched the issue in GitHub commit 8faa6ea692985dbe6ce10e1a3168e0bd60a723ba. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41886** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-54pp-c6pp-7fpx, https://github.com/tensorflow/tensorflow/commit/8faa6ea692985dbe6ce10e1a3168e0bd60a723ba | A-GOO-TENS-121222/234 |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. `tf.keras.losses.poisson` receives a `y_pred` and `y_true` that are passed through `functor::mul` in `BinaryOp`. If the resulting dimensions overflow an `int32`, TensorFlow will crash due to a size mismatch during broadcast assignment. We have patched the issue in | https://github.com/tensorflow/tensorflow/commit/c5b30379ba87cbe774b08ac50c1f6d36df4ebb7c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8fvv-46hw-vpg3 | A-GOO-TENS-121222/235 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | GitHub commit c5b30379ba87cbe774b08ac50c1f6d36df4ebb7c. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1 and 2.9.3, as these are also affected and still in supported range. However, we will not cherrypick this commit into TensorFlow 2.8.x, as it depends on Eigen behavior that changed between 2.8 and 2.9.<br>**CVE ID : CVE-2022-41887** | | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When running on GPU, `tf.image.generate_bounding_box_proposals` receives a `scores` input that must be of rank 4 but is not checked. We have patched the issue in GitHub commit cf35502463a88ca7185a99daa7031df60b3c1c98. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also | https://github.com/tensorflow/tensorflow/commit/cf35502463a88ca7185a99daa7031df60b3c1c98, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6x99-gv2v-q76v | A-GOO-TENS-121222/236 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected and still in supported range.<br>**CVE ID : CVE-2022-41888** | | |
| NULL Pointer Dereference | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If a list of quantized tensors is assigned to an attribute, the pywrap code fails to parse the tensor and returns a `nullptr`, which is not caught. An example can be seen in `tf.compat.v1.extract_volume_patches` by passing in quantized tensors as input `ksizes`. We have patched the issue in GitHub commit e9e95553e5411834d215e6770c81a83a3d0866ce. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41889** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xxcj-rhqg-m46g, https://github.com/tensorflow/tensorflow/commit/e9e95553e5411834d215e6770c81a83a3d0866ce | A-GOO-TENS-121222/237 |
| Incorrect Type Conversion or Cast | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `BCast::ToShape` is given input larger than an `int32`, it will | https://github.com/tensorflow/tensorflow/commit/8310bf8dd188ff780e7fc5324 | A-GOO-TENS-121222/238 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crash, despite being supposed to handle up to an `int64`. An example can be seen in `tf.experimental.numpy.outer` by passing in large input to the input `b`. We have patched the issue in GitHub commit 8310bf8dd188ff780e7fc53245058215a05bdbe5. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41890** | 5058215a05bdbe5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h246-cgh4-7475 | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListConcat` is given `element_shape=[]`, it results segmentation fault which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit fc33f3dc4c14051a83eec6535b608abe1d355fde. The fix will be included in TensorFlow 2.11. We | https://github.com/tensorflow/tensorflow/commit/fc33f3dc4c14051a83eec6535b608abe1d355fde, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-66vq-54fq-6jvv | A-GOO-TENS-121222/239 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41891** |  |  |
| Reachable Assertion | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `tf.raw_ops.TensorListResize` is given a nonscalar value for input `size`, it results `CHECK` fail which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 888e34b49009a4e734c27ab0c43b0b5102682c56. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41893** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-67pf-62xr-q35m, https://github.com/tensorflow/tensorflow/commit/888e34b49009a4e734c27ab0c43b0b5102682c56 | A-GOO-TENS-121222/240 |
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `MirrorPadGrad` is given outsize input `paddings`, TensorFlow will give a | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gq2j-cr96-gvqx, | A-GOO-TENS-121222/241 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | heap OOB error. We have patched the issue in GitHub commit 717ca98d8c3bba348ff62281fdf38dcb5ea1ec92. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41895** | https://github.com/tensorflow/tensorflow/commit/717ca98d8c3bba348ff62281fdf38dcb5ea1ec92 | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `ThreadUnsafeUnigramCandidateSampler` is given input `filterbank_channel_count` greater than the allowed max size, TensorFlow will crash. We have patched the issue in GitHub commit 39ec7eaf1428e90c37787e5b3fbd68ebd3c48860. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range. | https://github.com/tensorflow/tensorflow/commit/39ec7eaf1428e90c37787e5b3fbd68ebd3c48860, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rmg2-f698-wq35 | A-GOO-TENS-121222/242 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-41896** | | |
| Out-of-bounds Read | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `FractionMaxPoolGrad` is given outsize inputs `row_pooling_sequence` and `col_pooling_sequence`, TensorFlow will crash. We have patched the issue in GitHub commit d71090c3e5ca325bdf4b02eb236cfb3ee823e927. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41897** | https://github.com/tensorflow/tensorflow/commit/d71090c3e5ca325bdf4b02eb236cfb3ee823e927, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f2w8-jw48-fr7j | A-GOO-TENS-121222/243 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. If `SparseFillEmptyRowsGrad` is given empty inputs, TensorFlow will crash. We have patched the issue in GitHub commit af4a6a3c8b95022c351edae94560acc61253a1b8. The fix will be included in TensorFlow 2.11. We | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-hq7g-wwwp-q46h, https://github.com/tensorflow/tensorflow/commit/af4a6a3c8b95022c351edae9 | A-GOO-TENS-121222/244 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41898** | 4560acc61253a1b8 | |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. Inputs `dense_features` or `example_state_data` not of rank 2 will trigger a `CHECK` fail in `SdcaOptimizer`. We have patched the issue in GitHub commit 80ff197d03db2a70c6a111f97dcdacad1b0babfa. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41899** | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-27rc-728f-x5w2, https://github.com/tensorflow/tensorflow/commit/80ff197d03db2a70c6a111f97dcdacad1b0babfa | A-GOO-TENS-121222/245 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `sparse_matrix` that is not a matrix with a shape with rank 0 will trigger a `CHECK` fail in `tf.raw_ops.SparseMat | https://github.com/tensorflow/tensorflow/commit/f856d02e5322821aad155dad9b3acab1e9f5d693, https://githu | A-GOO-TENS-121222/246 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | rixNNZ`. We have patched the issue in GitHub commit f856d02e5322821aad155dad9b3acab1e9f5d693. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41901** | b.com/tensorflow/tensorflow/security/advisories/GHSA-g9fm-r5mm-rf9f | |
| Incorrect Calculation of Buffer Size | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When `tf.raw_ops.ResizeNearestNeighborGrad` is given a large `size` input, it overflows. We have patched the issue in GitHub commit 00c821af032ba9e5f5fa3fe14690c8d28a657624. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41907** | https://github.com/tensorflow/tensorflow/commit/00c821af032ba9e5f5fa3fe14690c8d28a657624,<br>https://github.com/tensorflow/tensorflow/security/advisories/GHSA-368v-7v32-52fx | A-GOO-TENS-121222/247 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `token` that is not a UTF-8 bytestring will trigger a `CHECK` fail in `tf.raw_ops.PyFunc`. We have patched the issue in GitHub commit 9f03a9d3bafe902c1e6beb105b2f24172f238645. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41908** | https://github.com/tensorflow/tensorflow/commit/9f03a9d3bafe902c1e6beb105b2f24172f238645, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv77-9g28-cwg3 | A-GOO-TENS-121222/248 |
| Improper Input Validation | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. An input `encoded` that is not a valid `CompositeTensorVariant` tensor will trigger a segfault in `tf.raw_ops.CompositeTensorVariantToComponents`. We have patched the issue in GitHub commits bf594d08d377dc6a3354d9fdb494b32d45f91971 and 660ce5a89eb6766834bdc303d2ab3902aef9 | https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rjx6-v474-2ch9, https://github.com/tensorflow/tensorflow/commit/660ce5a89eb6766834bdc303d2ab3902aef99d3d | A-GOO-TENS-121222/249 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 9d3d. The fix will be included in TensorFlow 2.11. We will also cherrypick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.<br>**CVE ID : CVE-2022-41909** | | |
| Incorrect Type Conversion or Cast | 18-Nov-2022 | 7.5 | TensorFlow is an open source platform for machine learning. When printing a tensor, we get it's data as a `const char*` array (since that's the underlying storage) and then we typecast it to the element type. However, conversions from `char` to `bool` are undefined if the `char` is not `0` or `1`, so sanitizers/fuzzers will crash. The issue has been patched in GitHub commit `1be74370327`. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.10.1, TensorFlow 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range. | https://github.com/tensorflow/tensorflow/commit/1be743703279782a357adbf9b77dcb994fe8b508, https://github.com/tensorflow/tensorflow/blob/807cae8a807960fd7ac2313cde73a11fc15e7942/tensorflow/core/framework/tensor.cc#L1200-L1227 | A-GOO-TENS-121222/250 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | **CVE ID : CVE-2022-41911** |  |  |
| **Vendor: google_forms_project** |  |  |  |  |  |
| **Product: google_forms** |  |  |  |  |  |
| Affected Version(s): * Up to (including) 0.95 |  |  |  |  |  |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Google Forms WordPress plugin through 0.95 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3834** | N/A | A-GOO-GOOG-121222/251 |
| **Vendor: Guitar-pro** |  |  |  |  |  |
| **Product: guitar_pro** |  |  |  |  |  |
| Affected Version(s): * Up to (excluding) 1.10.2 |  |  |  |  |  |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 16-Nov-2022 | 7.5 | Arobas Music Guitar Pro for iPad and iPhone before v1.10.2 allows attackers to perform directory traversal and download arbitrary files via a crafted web request.<br>**CVE ID : CVE-2022-43264** | N/A | A-GUI-GUIT-121222/252 |
| Improper Neutralization of | 16-Nov-2022 | 6.1 | A cross-site scripting (XSS) vulnerability in Arobas Music Guitar | N/A | A-GUI-GUIT-121222/253 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input During Web Page Generation ('Cross-site Scripting') | | | Pro for iPad and iPhone before v1.10.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the name of an uploaded file.<br>**CVE ID : CVE-2022-43263** | | |
| **Vendor: gunkastudios** | | | | | |
| **Product: login_block_ips** | | | | | |
| Affected Version(s): * Up to (including) 1.0.0 | | | | | |
| Authorization Bypass Through User-Controlled Key | 21-Nov-2022 | 7.5 | The function check_is_login_page() uses headers for the IP check, which can be easily spoofed.<br>**CVE ID : CVE-2022-1579** | https://wpscan.com/vulnerability/6f3d40fa-458b-44f0-9407-763e80b29668 | A-GUN-LOGI-121222/254 |
| **Vendor: gvectors** | | | | | |
| **Product: wpdiscuz** | | | | | |
| Affected Version(s): 7.4.2 | | | | | |
| Authorization Bypass Through User-Controlled Key | 18-Nov-2022 | 8.8 | Auth. (subscriber+) Insecure Direct Object References (IDOR) vulnerability in Comments – wpDiscuz plugin 7.4.2 on WordPress.<br>**CVE ID : CVE-2022-43492** | https://wordpress.org/plugins/wpdiscuz/#developers, https://patchstack.com/database/vulnerability/wpdiscuz/wordpress-comments-wpdiscuz-plugin-7-4-2-insecure-direct-object-references-idor- | A-GVE-WPDI-121222/255 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | vulnerability?_s_id=cve | |
| **Product: wpforo_forum** | | | | | |
| Affected Version(s): * Up to (including) 2.0.9 | | | | | |
| Cross-Site Request Forgery (CSRF) | 17-Nov-2022 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in wpForo Forum plugin <= 2.0.9 on WordPress.<br>**CVE ID : CVE-2022-40192** | https://patchstack.com/database/vulnerability/wpforo/wordpress-wpforo-forum-plugin-2-0-9-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | A-GVE-WPFO-121222/256 |
| Unrestricted Upload of File with Dangerous Type | 17-Nov-2022 | 8.8 | Auth. (subscriber+) Arbitrary File Upload vulnerability in wpForo Forum plugin <= 2.0.9 on WordPress.<br>**CVE ID : CVE-2022-40200** | https://patchstack.com/database/vulnerability/wpforo/wordpress-wpforo-forum-plugin-2-0-9-arbitrary-file-upload-vulnerability?_s_id=cve, https://wordpress.org/plugins/wpforo/#developers | A-GVE-WPFO-121222/257 |
| **Vendor: hashicorp** | | | | | |
| **Product: consul** | | | | | |
| Affected Version(s): From (including) 1.13.0 Up to (including) 1.13.3 | | | | | |
| Missing Authorization | 16-Nov-2022 | 7.5 | HashiCorp Consul and Consul Enterprise 1.13.0 up to 1.13.3 do not filter cluster filtering's imported nodes and services for | https://discuss.hashicorp.com/t/hcsec-2022-28-consul-cluster- | A-HAS-CONS-121222/258 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP or RPC endpoints used by the UI. Fixed in 1.14.0.<br>**CVE ID : CVE-2022-3920** | peering-leaks-imported-nodes-services-information/46946 | |
| **Vendor: hoosk** | | | | | |
| **Product: hoosk** | | | | | |
| Affected Version(s): 1.8.0 | | | | | |
| Unrestricted Upload of File with Dangerous Type | 16-Nov-2022 | 9.8 | An arbitrary file upload vulnerability in the /attachments component of Hoosk v1.8 allows attackers to execute arbitrary code via a crafted PHP file.<br>**CVE ID : CVE-2022-43234** | N/A | A-HOO-HOOS-121222/259 |
| **Vendor: hospital_management_center_project** | | | | | |
| **Product: hospital_management_center** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Nov-2022 | 9.8 | A vulnerability classified as critical has been found in Hospital Management Center. Affected is an unknown function of the file patient-info.php. The manipulation of the argument pt_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-213786 is the identifier assigned to this vulnerability. | N/A | A-HOS-HOSP-121222/260 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-4012** | | |
| Cross-Site Request Forgery (CSRF) | 16-Nov-2022 | 8.8 | A vulnerability classified as problematic was found in Hospital Management Center. Affected by this vulnerability is an unknown functionality of the file appointment.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-213787.<br>**CVE ID : CVE-2022-4013** | N/A | A-HOS-HOSP-121222/261 |
| **Vendor: hostel_searching_project** | | | | | |
| **Product: hostel_searching_project** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 9.8 | A vulnerability has been found in Hostel Searching Project and classified as critical. This vulnerability affects unknown code of the file view-property.php. The manipulation of the argument property_id leads to sql injection. The attack can be initiated remotely. The exploit has been | N/A | A-HOS-HOST-121222/262 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosed to the public and may be used. The identifier of this vulnerability is VDB-213844.<br>**CVE ID : CVE-2022-4051** | | |
| **Vendor: HP** | | | | | |
| **Product: nonstop_netbatch-plus** | | | | | |
| Affected Version(s): From (including) t9189h01 Up to (excluding) t9189h01\\^abw | | | | | |
| Improper Authentication | 22-Nov-2022 | 7.8 | A vulnerability in NetBatch-Plus software allows unauthorized access to the application. HPE has provided a workaround and fix. Please refer to HPE Security Bulletin HPESBNS04388 for details.<br>**CVE ID : CVE-2022-37931** | https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbns04388en_us | A-HP-NONS-121222/263 |
| Affected Version(s): From (including) t9189l01 Up to (excluding) t9189l01\\^aby | | | | | |
| Improper Authentication | 22-Nov-2022 | 7.8 | A vulnerability in NetBatch-Plus software allows unauthorized access to the application. HPE has provided a workaround and fix. Please refer to HPE Security Bulletin HPESBNS04388 for details.<br>**CVE ID : CVE-2022-37931** | https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbns04388en_us | A-HP-NONS-121222/264 |
| **Vendor: human_resource_management_system_project** | | | | | |
| **Product: human_resource_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Nov-2022 | 9.8 | Human Resource Management System v1.0 was discovered to contain a SQL injection vulnerability via the password parameter at /hrm/controller/login.php.<br>**CVE ID : CVE-2022-43262** | N/A | A-HUM-HUMA-121222/265 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 6.1 | Human Resource Management System v1.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability. This vulnerability is triggered via a crafted payload injected into an authentication error message.<br>**CVE ID : CVE-2022-45218** | N/A | A-HUM-HUMA-121222/266 |
| **Vendor: hustoj_project** | | | | | |
| **Product: hustoj** | | | | | |
| Affected Version(s): 22.09.22 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 6.1 | Hustoj 22.09.22 has a XSS Vulnerability in /admin/problem_judge.php.<br>**CVE ID : CVE-2022-42187** | N/A | A-HUS-HUST-121222/267 |
| **Vendor: ibericode** | | | | | |
| **Product: html_forms** | | | | | |
| Affected Version(s): * Up to (excluding) 1.3.25 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 28-Nov-2022 | 7.2 | The HTML Forms WordPress plugin before 1.3.25 does not properly properly escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users<br>**CVE ID : CVE-2022-3689** | N/A | A-IBE-HTML-121222/268 |
| **Vendor: IBM** | | | | | |
| **Product: business_automation_workflow** | | | | | |
| Affected Version(s): 20.0.0.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Multiple IBM Business Automation Workflow versions are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 233978.<br>**CVE ID : CVE-2022-38390** | https://www.ibm.com/support/pages/node/6839847, https://exchange.xforce.ibmcloud.com/vulnerabilities/233978 | A-IBM-BUSI-121222/269 |
| Affected Version(s): 20.0.0.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation | 17-Nov-2022 | 5.4 | Multiple IBM Business Automation Workflow versions are vulnerable to cross-site scripting. This vulnerability allows users to embed | https://www.ibm.com/support/pages/node/6839847, https://exchange.xforce.ibmcloud.com/v | A-IBM-BUSI-121222/270 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | 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: 233978.<br>**CVE ID : CVE-2022-38390** | ulnerabilities/233978 | |
| Affected Version(s): 22.0.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Multiple IBM Business Automation Workflow versions are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 233978.<br>**CVE ID : CVE-2022-38390** | https://www.ibm.com/support/pages/node/6839847, https://exchange.xforce.ibmcloud.com/vulnerabilities/233978 | A-IBM-BUSI-121222/271 |
| Affected Version(s): From (including) 18.0.0.0 Up to (including) 18.0.0.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Multiple IBM Business Automation Workflow versions are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality | https://www.ibm.com/support/pages/node/6839847, https://exchange.xforce.ibmcloud.com/vulnerabilities/233978 | A-IBM-BUSI-121222/272 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 233978.<br>**CVE ID : CVE-2022-38390** | | |
| Affected Version(s): From (including) 19.0.0.1 Up to (including) 19.0.0.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Multiple IBM Business Automation Workflow versions are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 233978.<br>**CVE ID : CVE-2022-38390** | https://www.ibm.com/support/pages/node/6839847, https://exchange.xforce.ibmcloud.com/vulnerabilities/233978 | A-IBM-BUSI-121222/273 |
| Affected Version(s): From (including) 21.0.1 Up to (including) 21.0.3.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Multiple IBM Business Automation Workflow versions are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted | https://www.ibm.com/support/pages/node/6839847, https://exchange.xforce.ibmcloud.com/vulnerabilities/233978 | A-IBM-BUSI-121222/274 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | session. IBM X-Force ID: 233978.<br>**CVE ID : CVE-2022-38390** | | |
| **Product: datapower_gateway** | | | | | |
| Affected Version(s): From (including) 10.0.1.0 Up to (including) 10.0.1.9 | | | | | |
| Insufficient Session Expiration | 22-Nov-2022 | 5.4 | IBM DataPower Gateway 10.0.3.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.9, 2018.4.1.0 through 2018.4.1.22, and 10.5.0.0 through 10.5.0.2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235527.<br>**CVE ID : CVE-2022-40228** | https://www.ibm.com/support/pages/node/6840759, https://exchange.xforce.ibmcloud.com/vulnerabilities/235527 | A-IBM-DATA-121222/275 |
| Affected Version(s): From (including) 10.0.3.0 Up to (including) 10.0.4.0 | | | | | |
| Insufficient Session Expiration | 22-Nov-2022 | 5.4 | IBM DataPower Gateway 10.0.3.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.9, 2018.4.1.0 through 2018.4.1.22, and 10.5.0.0 through 10.5.0.2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235527. | https://www.ibm.com/support/pages/node/6840759, https://exchange.xforce.ibmcloud.com/vulnerabilities/235527 | A-IBM-DATA-121222/276 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-40228** | | |
| Affected Version(s): From (including) 10.5.0.0 Up to (including) 10.5.0.2 | | | | | |
| Insufficient Session Expiration | 22-Nov-2022 | 5.4 | IBM DataPower Gateway 10.0.3.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.9, 2018.4.1.0 through 2018.4.1.22, and 10.5.0.0 through 10.5.0.2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235527.<br>**CVE ID : CVE-2022-40228** | https://www.ibm.com/support/pages/node/6840759, https://exchange.xforce.ibmcloud.com/vulnerabilities/235527 | A-IBM-DATA-121222/277 |
| Affected Version(s): From (including) 2018.4.1.0 Up to (including) 2018.4.1.22 | | | | | |
| Insufficient Session Expiration | 22-Nov-2022 | 5.4 | IBM DataPower Gateway 10.0.3.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.9, 2018.4.1.0 through 2018.4.1.22, and 10.5.0.0 through 10.5.0.2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235527.<br>**CVE ID : CVE-2022-40228** | https://www.ibm.com/support/pages/node/6840759, https://exchange.xforce.ibmcloud.com/vulnerabilities/235527 | A-IBM-DATA-121222/278 |
| **Product: infosphere_information_server** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): 11.7 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 16-Nov-2022 | 9.8 | IBM InfoSphere DataStage 11.7 is vulnerable to a command injection vulnerability due to improper neutralization of special elements. IBM X-Force ID: 236687.<br>**CVE ID : CVE-2022-40752** | https://www.ibm.com/support/pages/node/6833566, https://exchange.xforce.ibmcloud.com/vulnerabilities/236687 | A-IBM-INFO-121222/279 |
| **Product: infosphere_information_server_on_cloud** | | | | | |
| Affected Version(s): 11.7 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 16-Nov-2022 | 9.8 | IBM InfoSphere DataStage 11.7 is vulnerable to a command injection vulnerability due to improper neutralization of special elements. IBM X-Force ID: 236687.<br>**CVE ID : CVE-2022-40752** | https://www.ibm.com/support/pages/node/6833566, https://exchange.xforce.ibmcloud.com/vulnerabilities/236687 | A-IBM-INFO-121222/280 |
| **Product: i_access_client_solutions** | | | | | |
| Affected Version(s): From (including) 1.1.2 Up to (including) 1.1.4 | | | | | |
| Uncontrolled Search Path Element | 21-Nov-2022 | 6.7 | IBM i Access Family 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability. By placing a specially crafted file in a compromised folder, an attacker could | https://exchange.xforce.ibmcloud.com/vulnerabilities/236581, https://www.ibm.com/support/pages/node/6840359 | A-IBM-I_AC-121222/281 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236581.<br>**CVE ID : CVE-2022-40746** | | |
| Affected Version(s): From (including) 1.1.4.3 Up to (including) 1.1.9.0 | | | | | |
| Uncontrolled Search Path Element | 21-Nov-2022 | 6.7 | IBM i Access Family 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236581.<br>**CVE ID : CVE-2022-40746** | https://exchange.xforce.ibmcloud.com/vulnerabilities/236581, https://www.ibm.com/support/pages/node/6840359 | A-IBM-I_AC-121222/282 |
| **Product: partner_engagement_manager** | | | | | |
| Affected Version(s): 6.1.2 | | | | | |
| Insecure Storage of Sensitive Information | 16-Nov-2022 | 3.3 | IBM Sterling Partner Engagement Manager 2.0 allows encrypted storage of client data to be stored locally which can be read by another user on the system. IBM X-Force ID: 230424. | https://www.ibm.com/support/pages/node/6839751, https://exchange.xforce.ibmcloud.com/vulnerabilities/230424 | A-IBM-PART-121222/283 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-34354** | | |
| Affected Version(s): 6.2.0 | | | | | |
| Insecure Storage of Sensitive Information | 16-Nov-2022 | 3.3 | IBM Sterling Partner Engagement Manager 2.0 allows encrypted storage of client data to be stored locally which can be read by another user on the system. IBM X-Force ID: 230424.<br>**CVE ID : CVE-2022-34354** | https://www.ibm.com/support/pages/node/6839751, https://exchange.xforce.ibmcloud.com/vulnerabilities/230424 | A-IBM-PART-121222/284 |
| Affected Version(s): 6.2.1 | | | | | |
| Insecure Storage of Sensitive Information | 16-Nov-2022 | 3.3 | IBM Sterling Partner Engagement Manager 2.0 allows encrypted storage of client data to be stored locally which can be read by another user on the system. IBM X-Force ID: 230424.<br>**CVE ID : CVE-2022-34354** | https://www.ibm.com/support/pages/node/6839751, https://exchange.xforce.ibmcloud.com/vulnerabilities/230424 | A-IBM-PART-121222/285 |
| **Product: urbancode_deploy** | | | | | |
| Affected Version(s): From (including) 6.2.7.0 Up to (excluding) 6.2.7.18 | | | | | |
| Insufficiently Protected Credentials | 17-Nov-2022 | 4.9 | IBM UrbanCode Deploy (UCD) 6.2.7.0 through 6.2.7.17, 7.0.0.0 through 7.0.5.12, 7.1.0.0 through 7.1.2.8, and 7.2.0.0 through 7.2.3.1 could allow a user with administrative privileges including "Manage Security" permissions may be able to recover a | https://www.ibm.com/support/pages/node/6831907, https://exchange.xforce.ibmcloud.com/vulnerabilities/236601 | A-IBM-URBA-121222/286 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | credential previously saved for performing authenticated LDAP searches. IBM X-Force ID: 236601.<br>**CVE ID : CVE-2022-40751** | | |
| Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.0.5.13 | | | | | |
| Insufficiently Protected Credentials | 17-Nov-2022 | 4.9 | IBM UrbanCode Deploy (UCD) 6.2.7.0 through 6.2.7.17, 7.0.0.0 through 7.0.5.12, 7.1.0.0 through 7.1.2.8, and 7.2.0.0 through 7.2.3.1 could allow a user with administrative privileges including "Manage Security" permissions may be able to recover a credential previously saved for performing authenticated LDAP searches. IBM X-Force ID: 236601.<br>**CVE ID : CVE-2022-40751** | https://www.ibm.com/support/pages/node/6831907, https://exchange.xforce.ibmcloud.com/vulnerabilities/236601 | A-IBM-URBA-121222/287 |
| Affected Version(s): From (including) 7.1.0.0 Up to (excluding) 7.1.2.9 | | | | | |
| Insufficiently Protected Credentials | 17-Nov-2022 | 4.9 | IBM UrbanCode Deploy (UCD) 6.2.7.0 through 6.2.7.17, 7.0.0.0 through 7.0.5.12, 7.1.0.0 through 7.1.2.8, and 7.2.0.0 through 7.2.3.1 could allow a user with administrative privileges including "Manage Security" permissions may be able to recover a | https://www.ibm.com/support/pages/node/6831907, https://exchange.xforce.ibmcloud.com/vulnerabilities/236601 | A-IBM-URBA-121222/288 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | credential previously saved for performing authenticated LDAP searches. IBM X-Force ID: 236601.<br>**CVE ID : CVE-2022-40751** | | |
| Affected Version(s): From (including) 7.2.0.0 Up to (excluding) 7.2.3.2 | | | | | |
| Insufficiently Protected Credentials | 17-Nov-2022 | 4.9 | IBM UrbanCode Deploy (UCD) 6.2.7.0 through 6.2.7.17, 7.0.0.0 through 7.0.5.12, 7.1.0.0 through 7.1.2.8, and 7.2.0.0 through 7.2.3.1 could allow a user with administrative privileges including "Manage Security" permissions may be able to recover a credential previously saved for performing authenticated LDAP searches. IBM X-Force ID: 236601.<br>**CVE ID : CVE-2022-40751** | https://www.ibm.com/support/pages/node/6831907, https://exchange.xforce.ibmcloud.com/vulnerabilities/236601 | A-IBM-URBA-121222/289 |
| **Vendor: ikus-soft** | | | | | |
| **Product: rdiffweb** | | | | | |
| Affected Version(s): * Up to (including) 2.4.10 | | | | | |
| Missing Authentication for Critical Function | 16-Nov-2022 | 4.3 | Missing Authentication for Critical Function in GitHub repository ikus060/rdiffweb prior to 2.5.0a6.<br>**CVE ID : CVE-2022-4018** | https://github.com/ikus060/rdiffweb/commit/f2a32f2a9f3fb8be1a9432ac3d81d3aacdb13095, https://huntr.dev/bounties/5340c2f6- | A-IKU-RDIF-121222/290 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 0252-40f6-8929-cca5d64958a5 | |
| Affected Version(s): 2.5.0 | | | | | |
| Missing Authentication for Critical Function | 16-Nov-2022 | 4.3 | Missing Authentication for Critical Function in GitHub repository ikus060/rdiffweb prior to 2.5.0a6.<br>**CVE ID : CVE-2022-4018** | https://github.com/ikus060/rdiffweb/commit/f2a32f2a9f3fb8be1a9432ac3d81d3aacdb13095, https://huntr.dev/bounties/5340c2f6-0252-40f6-8929-cca5d64958a5 | A-IKU-RDIF-121222/291 |
| **Vendor: image_hover_effects_css3_project** | | | | | |
| **Product: image_hover_effects_css3** | | | | | |
| Affected Version(s): * Up to (including) 4.5 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Image Hover Effects Css3 WordPress plugin through 4.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3601** | N/A | A-IMA-IMAG-121222/292 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: inkthemes** | | | | | |
| **Product: ask_me** | | | | | |
| Affected Version(s): * Up to (excluding) 6.8.7 | | | | | |
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 4.7 | The has a CSRF vulnerability that allows the deletion of a post without using a nonce or prompting for confirmation.<br>**CVE ID : CVE-2022-3750** | https://wpscan.com/vulnerability/5019db80-0356-497d-b488-a26a5de78676 | A-INK-ASK_-121222/293 |
| **Vendor: installbuilder** | | | | | |
| **Product: installbuilder** | | | | | |
| Affected Version(s): * Up to (excluding) 22.10.0 | | | | | |
| Uncontrolled Search Path Element | 18-Nov-2022 | 7.3 | InstallBuilder Qt installers built with versions previous to 22.10 try to load DLLs from the installer binary parent directory when displaying popups. This may allow an attacker to plant a malicious DLL in the installer parent directory to allow executing code with the privileges of the installer (when the popup triggers the loading of the library). Exploiting these type of vulnerabilities generally require that an attacker has access to a vulnerable machine to plant the malicious DLL.<br>**CVE ID : CVE-2022-31694** | https://blog.installbuilder.com/2022/11/installbuilder-22100-released.html | A-INS-INST-121222/294 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: Iobit** | | | | | |
| **Product: iotransfer** | | | | | |
| Affected Version(s): 4.0 | | | | | |
| Unquoted Search Path or Element | 18-Nov-2022 | 7.8 | IOBit IOTransfer V4 is vulnerable to Unquoted Service Path.<br>**CVE ID : CVE-2022-37197** | N/A | A-IOB-IOTR-121222/295 |
| **Vendor: jeecg** | | | | | |
| **Product: jeecg_boot** | | | | | |
| Affected Version(s): 3.4.3 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 9.8 | Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/duplicate/check.<br>**CVE ID : CVE-2022-45206** | N/A | A-JEE-JEEC-121222/296 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 9.8 | Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component updateNullByEmptyString.<br>**CVE ID : CVE-2022-45207** | N/A | A-JEE-JEEC-121222/297 |
| Improper Neutralization of Special Elements used in an SQL Command | 25-Nov-2022 | 5.3 | Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/dict/queryTableData. | N/A | A-JEE-JEEC-121222/298 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | **CVE ID : CVE-2022-45205** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 4.3 | Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/user/putRecycleBin.<br>**CVE ID : CVE-2022-45208** | N/A | A-JEE-JEEC-121222/299 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 25-Nov-2022 | 4.3 | Jeecg-boot v3.4.3 was discovered to contain a SQL injection vulnerability via the component /sys/user/deleteRecycleBin.<br>**CVE ID : CVE-2022-45210** | N/A | A-JEE-JEEC-121222/300 |
| **Vendor: jeeng_push_notifications_project** | | | | | |
| **Product: jeeng_push_notifications** | | | | | |
| Affected Version(s): * Up to (excluding) 2.0.4 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Jeeng Push Notifications WordPress plugin before 2.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | N/A | A-JEE-JEEN-121222/301 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-3610** | | |
| **Vendor: Jetbrains** | | | | | |
| **Product: hub** | | | | | |
| Affected Version(s): * Up to (excluding) 2022.3.15181 | | | | | |
| Allocation of Resources Without Limits or Throttling | 18-Nov-2022 | 7.5 | In JetBrains Hub before 2022.3.15181 Throttling was missed when sending emails to a particular email address<br>**CVE ID : CVE-2022-45471** | https://www.jetbrains.com/privacy-security/issues-fixed/ | A-JET-HUB-121222/302 |
| **Vendor: jizhicms** | | | | | |
| **Product: jizhicms** | | | | | |
| Affected Version(s): 2.3.3 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 8.8 | Jizhicms v2.3.3 was discovered to contain a SQL injection vulnerability via the /Member/memberedit.html component.<br>**CVE ID : CVE-2022-44140** | N/A | A-JIZ-JIZH-121222/303 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 8.8 | Jizhicms v2.3.3 was discovered to contain a SQL injection vulnerability via the /index.php/admins/Fields/get_fields.html component.<br>**CVE ID : CVE-2022-45278** | N/A | A-JIZ-JIZH-121222/304 |
| **Vendor: joinmastodon** | | | | | |
| **Product: mastodon** | | | | | |
| Affected Version(s): 4.0.0 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Restriction of Excessive Authentication Attempts | 16-Nov-2022 | 9.8 | Improper Restriction of Excessive Authentication Attempts in GitHub repository mastodon/mastodon prior to 4.0.0.<br>**CVE ID : CVE-2022-2166** | https://huntr.dev/bounties/2f96f990-01c2-44ea-ae47-58bdb3aa455b, https://github.com/mastodon/mastodon/commit/21fd25a269cca742af431f0d13299e139f267346 | A-JOI-MAST-121222/305 |
| Affected Version(s): * Up to (including) 3.5.5 | | | | | |
| Improper Restriction of Excessive Authentication Attempts | 16-Nov-2022 | 9.8 | Improper Restriction of Excessive Authentication Attempts in GitHub repository mastodon/mastodon prior to 4.0.0.<br>**CVE ID : CVE-2022-2166** | https://huntr.dev/bounties/2f96f990-01c2-44ea-ae47-58bdb3aa455b, https://github.com/mastodon/mastodon/commit/21fd25a269cca742af431f0d13299e139f267346 | A-JOI-MAST-121222/306 |
| **Vendor: karmasis** | | | | | |
| **Product: infraskope_security_event_manager** | | | | | |
| Affected Version(s): * Up to (excluding) 7.10.00 | | | | | |
| N/A | 18-Nov-2022 | 7.5 | Karmasis informatics solutions Infraskope Security Event Manager product has an unauthenticated access which could allow an unauthenticated | https://www.usom.gov.tr/bildirim/tr-22-0691 | A-KAR-INFR-121222/307 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to obtain critical information.<br>**CVE ID : CVE-2022-24037** | | |
| N/A | 18-Nov-2022 | 7.5 | Karmasis informatics solutions Infraskope Security Event Manager product has an unauthenticated access which could allow an unauthenticated attacker to damage the page where the agents are listed.<br>**CVE ID : CVE-2022-24038** | https://www.usom.gov.tr/bildirim/tr-22-0691 | A-KAR-INFR-121222/308 |
| N/A | 16-Nov-2022 | 5.3 | Karmasis informatics solutions Infraskope Security Event Manager product has an unauthenticated access which could allow an unauthenticated attacker to modificate logs.<br>**CVE ID : CVE-2022-24036** | https://www.usom.gov.tr/bildirim/tr-22-0691 | A-KAR-INFR-121222/309 |
| **Vendor: keking** | | | | | |
| **Product: kkfileview** | | | | | |
| Affected Version(s): 4.1.0 | | | | | |
| Server-Side Request Forgery (SSRF) | 17-Nov-2022 | 7.5 | kkFileView v4.1.0 was discovered to contain a Server-Side Request Forgery (SSRF) via the component cn.keking.web.controller.OnlinePreviewController#getCorsFile. This vulnerability | N/A | A-KEK-KKFI-121222/310 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allows attackers to force the application to make arbitrary requests via injection of crafted URLs into the url parameter.<br>**CVE ID : CVE-2022-43140** | | |
| **Vendor: keyfactor** | | | | | |
| **Product: kefactor_ejbca** | | | | | |
| Affected Version(s): * Up to (excluding) 7.10.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | Keyfactor EJBCA before 7.10.0 allows XSS.<br>**CVE ID : CVE-2022-42954** | https://support.keyfactor.com/s/detail/a6x1Q000000CwCjQAK | A-KEY-KEFA-121222/311 |
| **Product: primekey_ejbca** | | | | | |
| Affected Version(s): * Up to (including) 7.9.0.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 5.4 | A stored XSS vulnerability was discovered in adminweb/ra/viewendentity.jsp in PrimeKey EJBCA through 7.9.0.2. A low-privilege user can store JavaScript in order to exploit a higher-privilege user.<br>**CVE ID : CVE-2022-39834** | https://support.keyfactor.com/s/detail/a6x1Q000000CwCoQAK | A-KEY-PRIM-121222/312 |
| **Vendor: keylime** | | | | | |
| **Product: keylime** | | | | | |
| Affected Version(s): * Up to (excluding) 6.5.1 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncaught Exception | 22-Nov-2022 | 5.1 | A vulnerability was found in keylime. This security issue happens in some circumstances, due to some improperly handled exceptions, there exists the possibility that a rogue agent could create errors on the verifier that stopped attestation attempts for that host leaving it in an attested state but not verifying that anymore.<br>**CVE ID : CVE-2022-3500** | https://github.com/keylime/keylime/pull/1128 | A-KEY-KEYL-121222/313 |
| **Vendor: kiwitcms** | | | | | |
| **Product: kiwi_tcms** | | | | | |
| Affected Version(s): * Up to (excluding) 11.6 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 5.4 | A stored XSS in a kiwi Test Plan can run malicious javascript which could be chained with an HTML injection to perform a UI redressing attack (clickjacking) and an HTML injection which disables the use of the history page.<br>**CVE ID : CVE-2022-4105** | https://huntr.dev/bounties/386417e9-0cd5-4d80-8137-b0fd5c30b8f8 ,<br>https://github.com/kiwitcms/kiwi/commit/a2b169ffdef1d7c1755bade8138578423b35011b | A-KIW-KIWI-121222/314 |
| **Vendor: klik-socialmediawebsite_project** | | | | | |
| **Product: klik-socialmediawebsite** | | | | | |
| Affected Version(s): 1.0.1 | | | | | |
| Improper Neutralizat | 22-Nov-2022 | 8.8 | KLiK SocialMediaWebsite | N/A | A-KLI-KLIK-121222/315 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ion of Special Elements used in an SQL Command ('SQL Injection') | | | version v1.0.1 is vulnerable to SQL Injection via the profile.php.<br>**CVE ID : CVE-2022-42098** | | |
| **Vendor: klik_project** | | | | | |
| **Product: klik** | | | | | |
| Affected Version(s): 1.0.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 29-Nov-2022 | 5.4 | KLiK SocialMediaWebsite Version 1.0.1 has XSS vulnerabilities that allow attackers to store XSS via location Forum Subject input.<br>**CVE ID : CVE-2022-42099** | N/A | A-KLI-KLIK-121222/316 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 29-Nov-2022 | 5.4 | KLiK SocialMediaWebsite Version 1.0.1 has XSS vulnerabilities that allow attackers to store XSS via location input reply-form.<br>**CVE ID : CVE-2022-42100** | N/A | A-KLI-KLIK-121222/317 |
| **Vendor: lancet_project** | | | | | |
| **Product: lancet** | | | | | |
| Affected Version(s): * Up to (excluding) 1.3.4 | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory | 17-Nov-2022 | 8.8 | Lancet is a general utility library for the go programming language. Affected versions are subject to a ZipSlip issue when using the fileutil package to unzip files. | https://github.com/duke-git/lancet/commit/f869a0a67098e92d24ddd913e188b32404fa72c9, | A-LAN-LANC-121222/318 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Path Traversal') | | | This issue has been addressed and a fix will be included in versions 2.1.10 and 1.3.4. Users are advised to upgrade. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-41920** | https://github.com/duke-git/lancet/commit/f133b32faa05eb93e66175d01827afa4b7094572, https://github.com/duke-git/lancet/security/advisories/GHSA-pp3f-xrw5-q5j4 | |
| Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.10 | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Nov-2022 | 8.8 | Lancet is a general utility library for the go programming language. Affected versions are subject to a ZipSlip issue when using the fileutil package to unzip files. This issue has been addressed and a fix will be included in versions 2.1.10 and 1.3.4. Users are advised to upgrade. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-41920** | https://github.com/duke-git/lancet/commit/f869a0a67098e92d24ddd913e188b32404fa72c9, https://github.com/duke-git/lancet/commit/f133b32faa05eb93e66175d01827afa4b7094572, https://github.com/duke-git/lancet/security/advisories/GHSA-pp3f-xrw5-q5j4 | A-LAN-LANC-121222/319 |
| **Vendor: LG** | | | | | |
| **Product: smart_share** | | | | | |
| Affected Version(s): - | | | | | |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncontrolled Search Path Element | 21-Nov-2022 | 7.8 | When LG SmartShare is installed, local privilege escalation is possible through DLL Hijacking attack. The LG ID is LVE-HOT-220005.<br>**CVE ID : CVE-2022-45422** | https://lgsecurity.lge.com/bulletins/pc | A-LG-SMAR-121222/320 |
| **Vendor: Libarchive** | | | | | |
| **Product: libarchive** | | | | | |
| Affected Version(s): 3.6.1 | | | | | |
| NULL Pointer Dereference | 22-Nov-2022 | 9.8 | In libarchive 3.6.1, the software does not check for an error after calling calloc function that can return with a NULL pointer if the function fails, which leads to a resultant NULL pointer dereference. NOTE: the discoverer cites this CWE-476 remark but third parties dispute the code-execution impact: "In rare circumstances, when NULL is equivalent to the 0x0 memory address and privileged code can access it, then writing or reading memory is possible, which may lead to code execution."<br>**CVE ID : CVE-2022-36227** | https://github.com/libarchive/libarchive/issues/1754, https://bugs.gentoo.org/882521 | A-LIB-LIBA-121222/321 |
| **Vendor: librenms** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: librenms** | | | | | |
| Affected Version(s): * Up to (excluding) 22.10.0 | | | | | |
| Insufficient Session Expiration | 20-Nov-2022 | 9.8 | Insufficient Session Expiration in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-4070** | https://github.com/librenms/librenms/commit/ce8e5f3d056829bfa7a845f9dc2757e21e419ddc, https://huntr.dev/bounties/72d426bb-b56e-4534-88ba-0d11381b0775 | A-LIB-LIBR-121222/322 |
| Deserialization of Untrusted Data | 20-Nov-2022 | 8.8 | Deserialization of Untrusted Data in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-3525** | https://huntr.dev/bounties/ed048e8d-87af-440a-a91f-be1e65a40330, https://github.com/librenms/librenms/commit/ae3925b09ad3c5d0f7a9d5a26ae2f2f778834948 | A-LIB-LIBR-121222/323 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Nov-2022 | 6.1 | Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-3516** | https://huntr.dev/bounties/734bb5eb-715c-4b64-bd33-280300a63748, https://github.com/librenms/librenms/commit/8e85 | A-LIB-LIBR-121222/324 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  |  | 698aa3aa4884c2f3d6c987542477eb64f07c |  |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Nov-2022 | 6.1 | Cross-site Scripting (XSS) - Generic in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-3561** | https://huntr.dev/bounties/7389e6eb-4bce-4b97-999d-d3b70d8cee34, https://github.com/librenms/librenms/commit/d86cbcd96d684e4de8dfa50b4490e4e02782d242 | A-LIB-LIBR-121222/325 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Nov-2022 | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-3562** | https://huntr.dev/bounties/bb9f76db-1314-44ae-9ccc-2b69679aa657, https://github.com/librenms/librenms/commit/43cb72549d90e338f902b359a83c23d3cb5a2645 | A-LIB-LIBR-121222/326 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Nov-2022 | 5.4 | Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-4067** | https://github.com/librenms/librenms/commit/8e85698aa3aa4884c2f3d6c987542477eb64f07c, https://huntr. | A-LIB-LIBR-121222/327 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | dev/bounties/3ca7023e-d95c-423f-9e9a-222a67a8ee72 | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Nov-2022 | 5.4 | A user is able to enable their own account if it was disabled by an admin while the user still holds a valid session. Moreover, the username is not properly sanitized in the admin user overview. This enables an XSS attack that enables an attacker with a low privilege user to execute arbitrary JavaScript in the context of an admin's account.<br>**CVE ID : CVE-2022-4068** | https://github.com/librenms/librenms/commit/09a2977adb8bc4b1db116c725d661160c930d3a1, https://huntr.dev/bounties/becfecc4-22a6-4f94-bf83-d6030b625fdc | A-LIB-LIBR-121222/328 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Nov-2022 | 4.8 | Cross-site Scripting (XSS) - Generic in GitHub repository librenms/librenms prior to 22.10.0.<br>**CVE ID : CVE-2022-4069** | https://github.com/librenms/librenms/commit/8383376f1355812e09ec0c2af67f6d46891b7ba7, https://huntr.dev/bounties/a9925d98-dac4-4c3c-835a-d93aeecfb2c5 | A-LIB-LIBR-121222/329 |
| **Vendor: lief-project** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: lief** | | | | | |
| Affected Version(s): 0.12.1 | | | | | |
| Out-of-bounds Write | 17-Nov-2022 | 6.5 | A heap buffer overflow in the LIEF::MachO::BinaryParser::parse_dyldinfo_generic_bind function of LIEF v0.12.1 allows attackers to cause a Denial of Service (DoS) via a crafted MachO file.<br>**CVE ID : CVE-2022-43171** | https://github.com/lief-project/LIEF/issues/782 | A-LIE-LIEF-121222/330 |
| **Vendor: lightning_network_daemon_project** | | | | | |
| **Product: lightning_network_daemon** | | | | | |
| Affected Version(s): * Up to (excluding) 0.15.4 | | | | | |
| Improper Input Validation | 17-Nov-2022 | 6.5 | Lightning Network Daemon (lnd) is an implementation of a lightning bitcoin overlay network node. All lnd nodes before version `v0.15.4` are vulnerable to a block parsing bug that can cause a node to enter a degraded state once encountered. In this degraded state, nodes can continue to make payments and forward HTLCs, and close out channels. Opening channels is prohibited, and also on chain transaction events will be undetected. This can cause loss of funds if a CSV expiry is researched during a breach attempt or a | https://github.com/lightningnetwork/lnd/issues/7096, https://github.com/lightningnetwork/lnd/pull/7098, https://github.com/lightningnetwork/lnd/security/advisories/GHSA-hc82-w9v8-83pr | A-LIG-LIGH-121222/331 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CLTV delta expires forgetting the funds in the HTLC. A patch is available in `lnd` version 0.15.4. Users are advised to upgrade. Users unable to upgrade may use the `lncli updatechanpolicy` RPC call to increase their CLTV value to a very high amount or increase their fee policies. This will prevent nodes from routing through your node, meaning that no pending HTLCs can be present.<br>**CVE ID : CVE-2022-39389** | | |
| **Vendor: linaro** | | | | | |
| **Product: lava** | | | | | |
| Affected Version(s): * Up to (excluding) 2022.11 | | | | | |
| Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | 18-Nov-2022 | 6.5 | In Linaro Automated Validation Architecture (LAVA) before 2022.11, users with valid credentials can submit crafted XMLRPC requests that cause a recursive XML entity expansion, leading to excessive use of memory on the server and a Denial of Service.<br>**CVE ID : CVE-2022-44641** | https://lists.lavasoftware.org/archives/list/lava-announce@lists.lavasoftware.org/thread/WHXGQMIZAPW3GCQEXYHC32N2ZAAAIYCY/ | A-LIN-LAVA-121222/332 |
| Affected Version(s): * Up to (excluding) 2022.11.1 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Control of Generation of Code ('Code Injection') | 18-Nov-2022 | 9.8 | In Linaro Automated Validation Architecture (LAVA) before 2022.11.1, remote code execution can be achieved through user-submitted Jinja2 template. The REST API endpoint for validating device configuration files in lava-server loads input as a Jinja2 template in a way that can be used to trigger remote code execution in the LAVA server.<br>**CVE ID : CVE-2022-45132** | https://lists.lavasoftware.org/archives/list/lava-announce@lists.lavasoftware.org/thread/WHXGQMIZAPW3GCQEXYHC32N2ZAAAIYCY/ | A-LIN-LAVA-121222/333 |
| **Vendor: Linux** | | | | | |
| **Product: linux_kernel** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 4.4 | NVIDIA CUDA Toolkit SDK contains a stack-based buffer overflow vulnerability in cuobjdump, where an unprivileged remote attacker could exploit this buffer overflow condition by persuading a local user to download a specially crafted corrupted file and execute cuobjdump against it locally, which may lead to a limited denial of service and some loss | https://nvidia.custhelp.com/app/answers/detail/a_id/5373 | A-LIN-LINU-121222/334 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of data integrity for the local user.<br>**CVE ID : CVE-2022-34667** | | |
| **Vendor: Linuxfoundation** | | | | | |
| **Product: kubevela** | | | | | |
| Affected Version(s): * Up to (excluding) 1.5.9 | | | | | |
| Server-Side Request Forgery (SSRF) | 16-Nov-2022 | 6.5 | KubeVela is an open source application delivery platform. Users using the VelaUX APIServer could be affected by this vulnerability. When using Helm Chart as the component delivery method, the request address of the warehouse is not restricted, and there is a blind SSRF vulnerability. Users who're using v1.6, please update the v1.6.1. Users who're using v1.5, please update the v1.5.8. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-39383** | https://github.com/kubevela/kubevela/security/advisories/GHSA-m5xf-x7q6-3rm7, https://github.com/kubevela/kubevela/pull/5000 | A-LIN-KUBE-121222/335 |
| Affected Version(s): From (including) 1.6.0 Up to (excluding) 1.6.2 | | | | | |
| Server-Side Request Forgery (SSRF) | 16-Nov-2022 | 6.5 | KubeVela is an open source application delivery platform. Users using the VelaUX APIServer could be affected by this vulnerability. | https://github.com/kubevela/kubevela/security/advisories/GHSA-m5xf-x7q6-3rm7, | A-LIN-KUBE-121222/336 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | When using Helm Chart as the component delivery method, the request address of the warehouse is not restricted, and there is a blind SSRF vulnerability. Users who're using v1.6, please update the v1.6.1. Users who're using v1.5, please update the v1.5.8. There are no known workarounds for this issue.<br>**CVE ID : CVE-2022-39383** | https://github.com/kubevela/kubevela/pull/5000 |  |
| **Product: pytorch** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 26-Nov-2022 | 9.8 | In PyTorch before trunk/89695, torch.jit.annotations.parse_type_line can cause arbitrary code execution because eval is used unsafely.<br>**CVE ID : CVE-2022-45907** | https://github.com/pytorch/pytorch/commit/767f6aa49fe20a2766b9843d01e3b7f7793df6a3 ,<br>https://github.com/pytorch/pytorch/issues/88868 | A-LIN-PYTO-121222/337 |
| **Vendor: Maarch** |  |  |  |  |  |
| **Product: maarch_rm** |  |  |  |  |  |
| Affected Version(s): 2.9 |  |  |  |  |  |
| Improper Restriction of Excessive Authentica | 23-Nov-2022 | 7.5 | Maarch RM 2.8.3 solution contains an improper restriction of excessive authentication | N/A | A-MAA-MAAR-121222/338 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| tion Attempts | | | attempts due to excessive verbose responses from the application. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to compromised accounts.<br>**CVE ID : CVE-2022-37772** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 6.5 | An authenticated SQL Injection vulnerability in the statistics page (/statistics/retrieve) of Maarch RM 2.8, via the filter parameter, allows the complete disclosure of all databases.<br>**CVE ID : CVE-2022-37773** | http://maarch.com | A-MAA-MAAR-121222/339 |
| Improper Authentication | 23-Nov-2022 | 5.3 | There is a broken access control vulnerability in the Maarch RM 2.8.3 solution. When accessing some specific document (pdf, email) from an archive, a preview is proposed by the application. This preview generates a URL including an md5 hash of the file accessed. The document's URL (https://{url}/tmp/{MD5 hash of the document}) is then | http://maarch.com | A-MAA-MAAR-121222/340 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | accessible without authentication.<br>**CVE ID : CVE-2022-37774** | | |
| Affected Version(s): From (including) 2.7 Up to (excluding) 2.8.6 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 6.5 | An authenticated SQL Injection vulnerability in the statistics page (/statistics/retrieve) of Maarch RM 2.8, via the filter parameter, allows the complete disclosure of all databases.<br>**CVE ID : CVE-2022-37773** | http://maarch.com | A-MAA-MAAR-121222/341 |
| Affected Version(s): From (including) 2.8 Up to (excluding) 2.8.6 | | | | | |
| Improper Restriction of Excessive Authentication Attempts | 23-Nov-2022 | 7.5 | Maarch RM 2.8.3 solution contains an improper restriction of excessive authentication attempts due to excessive verbose responses from the application. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to compromised accounts.<br>**CVE ID : CVE-2022-37772** | N/A | A-MAA-MAAR-121222/342 |
| Improper Authentication | 23-Nov-2022 | 5.3 | There is a broken access control vulnerability in the Maarch RM 2.8.3 solution. When accessing some specific document | http://maarch.com | A-MAA-MAAR-121222/343 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (pdf, email) from an archive, a preview is proposed by the application. This preview generates a URL including an md5 hash of the file accessed. The document's URL (https://{url}/tmp/{ MD5 hash of the document}) is then accessible without authentication.<br>**CVE ID : CVE-2022-37774** | | |
| **Vendor: maggioli** | | | | | |
| **Product: appalti_\&_contratti** | | | | | |
| Affected Version(s): 9.12.2 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 21-Nov-2022 | 9.8 | An issue was discovered in Appalti & Contratti 9.12.2. The target web applications are subject to multiple SQL Injection vulnerabilities, some of which executable even by unauthenticated users, as demonstrated by the GetListaEnti.do cfamm parameter.<br>**CVE ID : CVE-2022-44785** | N/A | A-MAG-APPA-121222/344 |
| N/A | 21-Nov-2022 | 8.8 | An issue was discovered in Appalti & Contratti 9.12.2. The target web applications LFS and DL229 expose a set of | N/A | A-MAG-APPA-121222/345 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  | 🟧 | services provided by the Axis 1.4 instance, embedded directly into the applications, as hinted by the WEB-INF/web.xml file leaked through Local File Inclusion. Among the exposed services, there is the Axis AdminService, which, through the default configuration, should normally be accessible only by the localhost. Nevertheless, by trying to access the mentioned service, both in LFS and DL229, the service can actually be reached even by remote users, allowing creation of arbitrary services on the server side. When an attacker can reach the AdminService, they can use it to instantiate arbitrary services on the server. The exploit procedure is well known and described in Generic AXIS-SSRF exploitation. Basically, the attack consists of writing a JSP page inside the root directory of the web application, through the org.apache.axis.handlers.LogHandler class. |  |  |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-44784** | | |
| N/A | 21-Nov-2022 | 7.5 | An issue was discovered in Appalti & Contratti 9.12.2. The target web applications allow Local File Inclusion in any page relying on the href parameter to specify the JSP page to be rendered. This affects ApriPagina.do POST and GET requests to each application.<br>**CVE ID : CVE-2022-44786** | N/A | A-MAG-APPA-121222/346 |
| Session Fixation | 21-Nov-2022 | 6.5 | An issue was discovered in Appalti & Contratti 9.12.2. It allows Session Fixation. When a user logs in providing a JSESSIONID cookie that is issued by the server at the first visit, the cookie value is not updated after a successful login.<br>**CVE ID : CVE-2022-44788** | N/A | A-MAG-APPA-121222/347 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 6.1 | An issue was discovered in Appalti & Contratti 9.12.2. The web applications are vulnerable to a Reflected Cross-Site Scripting issue. The idPagina parameter is reflected inside the server response | N/A | A-MAG-APPA-121222/348 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | without any HTML encoding, resulting in XSS when the victim moves the mouse pointer inside the page. As an example, the onmouseenter attribute is not sanitized.<br>**CVE ID : CVE-2022-44787** | | |
| **Vendor: Maradns** | | | | | |
| **Product: maradns** | | | | | |
| Affected Version(s): * Up to (excluding) 3.4.03 | | | | | |
| Operation on a Resource after Expiration or Release | 19-Nov-2022 | 7.5 | An issue was discovered in MaraDNS Deadwood through 3.5.0021 that allows variant V1 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.<br>**CVE ID : CVE-2022-30256** | https://maradns.samiam.org/, https://maradns.samiam.org/security.html#CVE-2022-30256 | A-MAR-MARA-121222/349 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.0022 | | | | | |
| Operation on a Resource after Expiration or Release | 19-Nov-2022 | 7.5 | An issue was discovered in MaraDNS Deadwood through 3.5.0021 that allows variant V1 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.<br>**CVE ID : CVE-2022-30256** | https://maradns.samiam.org/, https://maradns.samiam.org/security.html#CVE-2022-30256 | A-MAR-MARA-121222/350 |
| **Vendor: Matrix** | | | | | |
| **Product: synapse** | | | | | |
| Affected Version(s): * Up to (excluding) 1.53.0 | | | | | |
| Uncontrolled Resource Consumption | 22-Nov-2022 | 5.3 | Synapse before 1.52.0 with URL preview functionality enabled will attempt to generate URL previews for media stream URLs without properly limiting connection time. Connections will only be terminated after | https://github.com/matrix-org/synapse/security/advisories/GHSA-4822-jvwx-w47h, https://github.com/matrix- | A-MAT-SYNA-121222/351 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | `max_spider_size` (default: 10M) bytes have been downloaded, which can in some cases lead to long-lived connections towards the streaming media server (for instance, Icecast). This can cause excessive traffic and connections toward such servers if their stream URL is, for example, posted to a large room with many Synapse instances with URL preview enabled. Version 1.52.0 implements a timeout mechanism which will terminate URL preview connections after 30 seconds. Since generating URL previews for media streams is not supported and always fails, 1.53.0 additionally implements an allow list for content types for which Synapse will even attempt to generate a URL preview. Upgrade to 1.53.0 to fully resolve the issue. As a workaround, turn off URL preview functionality by setting `url_preview_enabled: | org/synapse/pull/11936, https://github.com/matrix-org/synapse/pull/11784 |  |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | false` in the Synapse configuration file.<br>**CVE ID : CVE-2022-41952** | | |
| **Vendor: mattermost** | | | | | |
| **Product: mattermost** | | | | | |
| Affected Version(s): - | | | | | |
| Allocation of Resources Without Limits or Throttling | 23-Nov-2022 | 6.5 | A denial-of-service vulnerability in the Mattermost Playbooks plugin allows an authenticated user to crash the server via multiple large requests to one of the Playbooks API endpoints.<br>**CVE ID : CVE-2022-4019** | https://mattermost.com/security-updates/ | A-MAT-MATT-121222/352 |
| Allocation of Resources Without Limits or Throttling | 23-Nov-2022 | 6.5 | A denial-of-service vulnerability in the Mattermost allows an authenticated user to crash the server via multiple requests to one of the API endpoints which could fetch a large amount of data.<br>**CVE ID : CVE-2022-4045** | https://mattermost.com/security-updates/ | A-MAT-MATT-121222/353 |
| Affected Version(s): * Up to (excluding) 7.4 | | | | | |
| Allocation of Resources Without Limits or Throttling | 23-Nov-2022 | 6.5 | A denial-of-service vulnerability in Mattermost allows an authenticated user to crash the server via multiple large autoresponder messages. | https://mattermost.com/security-updates/ | A-MAT-MATT-121222/354 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-4044** | | |
| **Vendor: Maxfoundry** | | | | | |
| **Product: media_library_folders** | | | | | |
| Affected Version(s): * Up to (excluding) 7.1.2 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Media Library Folders plugin <= 7.1.1 on WordPress.<br>**CVE ID : CVE-2022-41634** | https://wordpress.org/plugins/media-library-plus/#developers, https://patchstack.com/database/vulnerability/media-library-plus/wordpress-media-library-folders-plugin-7-1-1-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | A-MAX-MEDI-121222/355 |
| **Vendor: Mcafee** | | | | | |
| **Product: total_protection** | | | | | |
| Affected Version(s): * Up to (excluding) 16.0.49 | | | | | |
| Uncontrolled Search Path Element | 23-Nov-2022 | 7.8 | McAfee Total Protection prior to version 16.0.49 contains an uncontrolled search path element vulnerability due to the use of a variable pointing to a subdirectory that may be controllable by an unprivileged user. | https://www.mcafee.com/support/?articleId=TS103348&page=shell&shell=article-view | A-MCA-TOTA-121222/356 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | This may have allowed the unprivileged user to execute arbitrary code with system privileges.<br>**CVE ID : CVE-2022-43751** | | |
| **Vendor: media_library_assistant_project** | | | | | |
| **Product: media_library_assistant** | | | | | |
| Affected Version(s): * Up to (excluding) 3.01 | | | | | |
| Insertion of Sensitive Information into Log File | 18-Nov-2022 | 5.3 | Unauthenticated Error Log Disclosure vulnerability in Media Library Assistant plugin <= 3.00 on WordPress.<br>**CVE ID : CVE-2022-41618** | https://wordpress.org/plugins/media-library-assistant/#developers, https://patchstack.com/database/vulnerability/media-library-assistant/wordpress-media-library-assistant-plugin-3-00-unauthenticated-error-log-disclosure-vulnerability?_s_id=cve | A-MED-MEDI-121222/357 |
| **Vendor: metagauss** | | | | | |
| **Product: profilegrid** | | | | | |
| Affected Version(s): * Up to (including) 5.1.6 | | | | | |
| Improper Neutralization of Formula Elements | 17-Nov-2022 | 8.8 | Auth. (subscriber+) CSV Injection vulnerability in ProfileGrid plugin <= 5.1.6 on WordPress. | https://patchstack.com/database/vulnerability/profilegrid-user-profiles- | A-MET-PROF-121222/358 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| in a CSV File | | | **CVE ID : CVE-2022-41791** | groups-and-communities/wordpress-profilegrid-plugin-5-1-6-csv-injection-vulnerability?_s_id=cve | |
| **Vendor: Microfocus** | | | | | |
| **Product: filr** | | | | | |
| Affected Version(s): * Up to (excluding) 4.3.1.1 | | | | | |
| N/A | 21-Nov-2022 | 5.3 | A vulnerability has been identified in Micro Focus Filr in versions prior to 4.3.1.1. The vulnerability could be exploited to allow a remote unauthenticated attacker to enumerate valid users of the system. Remote unauthenticated user enumeration. This issue affects: Micro Focus Filr versions prior to 4.3.1.1.<br>**CVE ID : CVE-2022-38755** | https://portal.microfocus.com/s/article/KM000011886?language=en_US | A-MIC-FILR-121222/359 |
| **Vendor: Microsoft** | | | | | |
| **Product: edge** | | | | | |
| Affected Version(s): * Up to (excluding) 107.0.1418.62 | | | | | |
| Out-of-bounds Write | 25-Nov-2022 | 9.6 | Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to | https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_24.html | A-MIC-EDGE-121222/360 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)<br>**CVE ID : CVE-2022-4135** | | |
| **Product: edge_chromium** | | | | | |
| Affected Version(s): * Up to (excluding) 107.0.5304.150 | | | | | |
| Out-of-bounds Write | 25-Nov-2022 | 9.6 | Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)<br>**CVE ID : CVE-2022-4135** | https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_24.html | A-MIC-EDGE-121222/361 |
| **Vendor: Microweber** | | | | | |
| **Product: microweber** | | | | | |
| Affected Version(s): 1.2.15 | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 22-Nov-2022 | 8.8 | Microweber v1.2.15 was discovered to allow attackers to perform an account takeover via a host header injection attack.<br>**CVE ID : CVE-2022-33012** | N/A | A-MIC-MICR-121222/362 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: miniorange** | | | | | |
| **Product: google_authenticator** | | | | | |
| Affected Version(s): * Up to (excluding) 5.6.2 | | | | | |
| N/A | 18-Nov-2022 | 8.8 | Broken Access Control vulnerability in miniOrange's Google Authenticator plugin <= 5.6.1 on WordPress.<br>**CVE ID : CVE-2022-42461** | https://patchstack.com/database/vulnerability/miniorange-2-factor-authentication/wordpress-miniorange-s-google-authenticator-plugin-5-6-1-broken-access-control-vulnerability?_s_id=cve | A-MIN-GOOG-121222/363 |
| **Product: wordpress_rest_api_authentication** | | | | | |
| Affected Version(s): * Up to (including) 2.4.0 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in REST API Authentication plugin <= 2.4.0 on WordPress.<br>**CVE ID : CVE-2022-45073** | https://patchstack.com/database/vulnerability/wp-rest-api-authentication/wordpress-rest-api-authentication-plugin-2-4-0-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | A-MIN-WORD-121222/364 |
| **Vendor: Mitel** | | | | | |
| **Product: micollab** | | | | | |
| Affected Version(s): * Up to (including) 9.6.0.105 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Authorization | 22-Nov-2022 | 9.8 | The web conferencing component of Mitel MiCollab through 9.6.0.13 could allow an unauthenticated attacker to upload arbitrary scripts due to improper authorization controls. A successful exploit could allow remote code execution within the context of the application.<br>**CVE ID : CVE-2022-41326** | https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0009, https://www.mitel.com/support/security-advisories | A-MIT-MICO-121222/365 |
| **Product: mivoice_connect** | | | | | |
| Affected Version(s): * Up to (excluding) 19.3 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 22-Nov-2022 | 6.8 | A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker with internal network access to conduct a command-injection attack, due to insufficient restriction of URL parameters.<br>**CVE ID : CVE-2022-40765** | https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0007 | A-MIT-MIVO-121222/366 |
| Improper Control of Generation of Code ('Code Injection') | 22-Nov-2022 | 6.8 | The Director database component of MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker to conduct a code-injection attack via crafted data due to insufficient | https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0008, | A-MIT-MIVO-121222/367 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | restrictions on the database data type.<br>**CVE ID : CVE-2022-41223** | https://www.mitel.com/support/security-advisories | |
| Affected Version(s): 19.3 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 22-Nov-2022 | 6.8 | A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker with internal network access to conduct a command-injection attack, due to insufficient restriction of URL parameters.<br>**CVE ID : CVE-2022-40765** | https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0007 | A-MIT-MIVO-121222/368 |
| Improper Control of Generation of Code ('Code Injection') | 22-Nov-2022 | 6.8 | The Director database component of MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker to conduct a code-injection attack via crafted data due to insufficient restrictions on the database data type.<br>**CVE ID : CVE-2022-41223** | https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0008, https://www.mitel.com/support/security-advisories | A-MIT-MIVO-121222/369 |
| **Vendor: Mitsubishielectric** | | | | | |
| **Product: gx_works3** | | | | | |
| Affected Version(s): From (including) 1.000a Up to (including) 1.011m | | | | | |
| Cleartext Storage of Sensitive | 25-Nov-2022 | 7.5 | Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric GX Works3 versions | https://www.mitsubishielectric.com/en/psirt/vulnera | A-MIT-GX_W-121222/370 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information |  |  | 1.086Q and prior allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthorized users may view or execute programs illegally.<br>**CVE ID : CVE-2022-29826** | bility/pdf/2022-015_en.pdf |  |
| Affected Version(s): From (including) 1.015r Up to (including) 1.086q |  |  |  |  |  |
| Cleartext Storage of Sensitive Information | 25-Nov-2022 | 7.5 | Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric GX Works3 versions 1.086Q and prior allows a remote unauthenticated attacker to disclose sensitive information. As a result, unauthorized users may view or execute programs illegally.<br>**CVE ID : CVE-2022-29826** | https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-015_en.pdf | A-MIT-GX_W-121222/371 |
| **Vendor: Moodle** |  |  |  |  |  |
| **Product: moodle** |  |  |  |  |  |
| Affected Version(s): From (including) 3.11.0 Up to (excluding) 3.11.11 |  |  |  |  |  |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 6.1 | A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to | http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76091, https://moodle.org/mod/fo | A-MOO-MOOD-121222/372 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.<br>**CVE ID : CVE-2022-45150** | rum/discuss.php?d=440770 |  |
| Cross-Site Request Forgery (CSRF) | 23-Nov-2022 | 5.4 | A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks. | https://moodle.org/mod/forum/discuss.php?d=440769, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75862 | A-MOO-MOOD-121222/373 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-45149** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.<br>**CVE ID : CVE-2022-45151** | https://moodle.org/mod/forum/discuss.php?d=440771, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76131 | A-MOO-MOOD-121222/374 |
| Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.18 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 6.1 | A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive | http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76091, https://moodle.org/mod/forum/discuss.php?d=440770 | A-MOO-MOOD-121222/375 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information and modification of web pages.<br>**CVE ID : CVE-2022-45150** | | |
| Cross-Site Request Forgery (CSRF) | 23-Nov-2022 | 5.4 | A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.<br>**CVE ID : CVE-2022-45149** | https://moodle.org/mod/forum/discuss.php?d=440769, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75862 | A-MOO-MOOD-121222/376 |
| Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.5 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 6.1 | A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can | http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76091, https://moodle.org/mod/fo | A-MOO-MOOD-121222/377 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.<br>**CVE ID : CVE-2022-45150** | rum/discuss.php?d=440770 | |
| Cross-Site Request Forgery (CSRF) | 23-Nov-2022 | 5.4 | A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site | https://moodle.org/mod/forum/discuss.php?d=440769,<br>http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75862 | A-MOO-MOOD-121222/378 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | request forgery attacks.<br>**CVE ID : CVE-2022-45149** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.<br>**CVE ID : CVE-2022-45151** | https://moodle.org/mod/forum/discuss.php?d=440771, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76131 | A-MOO-MOOD-121222/379 |
| **Vendor: Mozilla** | | | | | |
| **Product: firefox** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Resource Shutdown or Release | 19-Nov-2022 | 8.2 | A vulnerability was found in davidmoreno onion. It has been rated as problematic. Affected by this issue is the function onion_response_flush of the file src/onion/response.c of the component Log Handler. The manipulation leads to allocation of resources. The name of the patch is de8ea938342b36c28024fd8393ebc27b8442a161. It is | https://github.com/davidmoreno/onion/commit/de8ea938342b36c28024fd8393ebc27b8442a161, https://github.com/davidmoreno/onion/pull/308 | A-MOZ-FIRE-121222/380 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-214028.<br>**CVE ID : CVE-2022-4066** | | |
| **Vendor: msi** | | | | | |
| **Product: center** | | | | | |
| Affected Version(s): 1.0.41.0 | | | | | |
| Insufficient Verification of Data Authenticity | 28-Nov-2022 | 8.8 | An issue in the component MSI.TerminalServer.exe of MSI Center v1.0.41.0 allows attackers to escalate privileges via a crafted TCP packet.<br>**CVE ID : CVE-2022-31877** | http://msi.com | A-MSI-CENT-121222/381 |
| **Vendor: muffingroup** | | | | | |
| **Product: betheme** | | | | | |
| Affected Version(s): * Up to (excluding) 26.6 | | | | | |
| Deserialization of Untrusted Data | 17-Nov-2022 | 8.8 | Auth. (subscriber+) PHP Object Injection vulnerability in Betheme theme <= 26.5.1.4 on WordPress.<br>**CVE ID : CVE-2022-45077** | https://patchstack.com/database/vulnerability/betheme/wordpress-betheme-theme-26-5-1-4-auth-php-object-injection-vulnerability?_s_id=cve, https://themeforest.net/item/betheme-responsive-multipurpose- | A-MUF-BETH-121222/382 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | wordpress-theme/7758048 | |
| Affected Version(s): * Up to (including) 26.6.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 5.4 | Auth. (subscriber+) Stored Cross-Site Scripting (XSS) in Muffingroup Betheme theme <= 26.6.1 on WordPress.<br>**CVE ID : CVE-2022-45363** | N/A | A-MUF-BETH-121222/383 |
| **Vendor: Mybb** | | | | | |
| **Product: mybb** | | | | | |
| Affected Version(s): * Up to (excluding) 1.8.32 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 6.1 | MyBB 1.8.31 has a Cross-site scripting (XSS) vulnerability in the visual MyCode editor (SCEditor) allows remote attackers to inject HTML via user input or stored data<br>**CVE ID : CVE-2022-43707** | https://github.com/mybb/mybb/security/advisories/GHSA-6vpw-m83q-27px | A-MYB-MYBB-121222/384 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 6.1 | MyBB 1.8.31 has a (issue 2 of 2) cross-site scripting (XSS) vulnerabilities in the post Attachments interface allow attackers to inject HTML by persuading the user to upload a file with specially crafted name<br>**CVE ID : CVE-2022-43708** | https://github.com/mybb/mybb/security/advisories/GHSA-p9m7-9qv4-x93w | A-MYB-MYBB-121222/385 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22-Nov-2022 | 4.9 | MyBB 1.8.31 has a SQL injection vulnerability in the Admin CP's Users module allows remote authenticated users to modify the query string via direct user input or stored search filter settings.<br>**CVE ID : CVE-2022-43709** | https://github.com/mybb/mybb/security/advisories/GHSA-ggp5-454p-867v | A-MYB-MYBB-121222/386 |
| **Vendor: my_wpdb_project** | | | | | |
| **Product: my_wpdb** | | | | | |
| Affected Version(s): * Up to (excluding) 2.5 | | | | | |
| Cross-Site Request Forgery (CSRF) | 21-Nov-2022 | 8.8 | The My wpdb WordPress plugin before 2.5 is missing CSRF check when running SQL queries, which could allow attacker to make a logged in admin run arbitrary SQL query via a CSRF attack<br>**CVE ID : CVE-2022-1578** | https://wpscan.com/vulnerability/c280da92-4ac2-43ea-93a2-6c583b79b98b | A-MY_-MY_W-121222/387 |
| **Vendor: ndk-design** | | | | | |
| **Product: ndkadvancedcustomizationfields** | | | | | |
| Affected Version(s): * Up to (including) 3.5.0 | | | | | |
| Server-Side Request Forgery (SSRF) | 22-Nov-2022 | 9.1 | ndk design NdkAdvancedCustomizationFields 3.5.0 is vulnerable to Server-side request forgery (SSRF) via rotateimg.php.<br>**CVE ID : CVE-2022-40842** | N/A | A-NDK-NDKA-121222/388 |
| **Vendor: Nvidia** | | | | | |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: cloud_gaming_guest** | | | | | |
| Affected Version(s): * Up to (excluding) 515.65.01 | | | | | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/389 |
| Affected Version(s): * Up to (excluding) 516.94 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/390 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-31606** | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/391 |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/392 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/393 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/394 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null- | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/395 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-CLOU-121222/396 |
| **Product: cuda_toolkit** | | | | | |
| Affected Version(s): * Up to (excluding) 11.8 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 4.4 | NVIDIA CUDA Toolkit SDK contains a stack-based buffer overflow vulnerability in cuobjdump, where an unprivileged remote attacker could exploit this buffer overflow condition by persuading a local user to download a specially crafted corrupted file and execute cuobjdump against it locally, which may lead to a limited denial of service and some loss of data integrity for the local user. | https://nvidia.custhelp.com/app/answers/detail/a_id/5373 | A-NVI-CUDA-121222/397 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-34667** | | |
| **Product: gpu_display_driver** | | | | | |
| Affected Version(s): From (including) 390 Up to (excluding) 390.154 | | | | | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/398 |
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/399 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/400 |
| Affected Version(s): From (including) 450 Up to (excluding) 450.203.03 | | | | | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/401 |
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/402 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/403 |
| Affected Version(s): From (including) 451.48 Up to (excluding) 453.64 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/404 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/405 |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/406 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/407 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/408 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null- | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/409 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/410 |
| Affected Version(s): From (including) 470 Up to (excluding) 470.141.03 | | | | | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/411 |
| Improper Preservation of | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus | https://nvidia.custhelp.com/app/answers | A-NVI-GPU_-121222/412 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Permissions | | | configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | /detail/a_id/5383 | |
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/413 |
| Affected Version(s): From (including) 471.11 Up to (excluding) 472.81 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of- | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/414 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/415 |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/416 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/417 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/418 |
| NULL Pointer | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows | https://nvidia.custhelp.com | A-NVI-GPU_-121222/419 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Dereference |  |  | contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | /app/answers/detail/a_id/5383 |  |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/420 |
| Affected Version(s): From (including) 471.11 Up to (excluding) 473.81 |  |  |  |  |  |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/421 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/422 |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/423 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-31617** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/424 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/425 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the | https://nvidia.custhelp.com/app/answers | A-NVI-GPU_-121222/426 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | /detail/a_id/5383 | |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/427 |
| Affected Version(s): From (including) 510 Up to (excluding) 510.85.02 | | | | | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/428 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/429 |
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/430 |
| Affected Version(s): From (including) 511.09 Up to (excluding) 513.46 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/431 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/432 |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/433 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/434 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/435 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure.<br>**CVE ID : CVE-2022-31616** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/436 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/437 |
| Affected Version(s): From (including) 515 Up to (excluding) 515.65.01 | | | | | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/438 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | | |
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/439 |
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/440 |
| Affected Version(s): From (including) 516.25 Up to (excluding) 516.94 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/441 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/442 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/443 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/444 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/445 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/446 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-GPU_-121222/447 |
| **Product: rtx** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-RTX-121222/448 |
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-RTX-121222/449 |
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-RTX-121222/450 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | | |
| **Product: studio** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/451 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/452 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/453 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/454 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | internal kernel information.<br>**CVE ID : CVE-2022-31612** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/455 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/456 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null- | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-STUD-121222/457 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | | |
| **Product: virtual_gpu** | | | | | |
| Affected Version(s): 14.0 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/458 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/459 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/460 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/461 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-31612** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/462 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/463 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/464 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | | |
| Affected Version(s): From (including) 11.0 Up to (excluding) 11.8 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/465 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/466 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/467 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/468 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/469 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/470 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/471 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-34665** | | |
| Affected Version(s): From (including) 13.0 Up to (excluding) 13.3 | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/472 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/473 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/474 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/475 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/476 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/477 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | A-NVI-VIRT-121222/478 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-34665** | | |
| **Vendor: octopus** | | | | | |
| **Product: octopus_server** | | | | | |
| Affected Version(s): From (including) 2022.2.6729 Up to (excluding) 2022.2.7965 | | | | | |
| Insertion of Sensitive Information into Log File | 25-Nov-2022 | 7.5 | In affected versions of Octopus Server it is possible for target discovery to print certain values marked as sensitive to log files in plaint-text in when verbose logging is enabled.<br>**CVE ID : CVE-2022-2721** | https://advisories.octopus.com/post/2022/sa2022-24/ | A-OCT-OCTO-121222/479 |
| Affected Version(s): From (including) 2022.3.348 Up to (excluding) 2022.3.9163 | | | | | |
| Insertion of Sensitive Information into Log File | 25-Nov-2022 | 7.5 | In affected versions of Octopus Server it is possible for target discovery to print certain values marked as sensitive to log files in plaint-text in when verbose logging is enabled.<br>**CVE ID : CVE-2022-2721** | https://advisories.octopus.com/post/2022/sa2022-24/ | A-OCT-OCTO-121222/480 |
| **Vendor: okfn** | | | | | |
| **Product: ckan** | | | | | |
| Affected Version(s): * Up to (excluding) 2.8.12 | | | | | |
| Improper Authentication | 22-Nov-2022 | 8.8 | CKAN through 2.9.6 account takeovers by unauthenticated users when an existing user id is sent via an HTTP POST request. This allows a user to take over an existing | https://ckan.org/,<br>https://ckan.org/blog/get-latest-patch-releases-your-ckan-site-october-2022 | A-OKF-CKAN-121222/481 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | account including superuser accounts.<br>**CVE ID : CVE-2022-43685** | | |
| Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.7 | | | | | |
| Improper Authentication | 22-Nov-2022 | 8.8 | CKAN through 2.9.6 account takeovers by unauthenticated users when an existing user id is sent via an HTTP POST request. This allows a user to take over an existing account including superuser accounts.<br>**CVE ID : CVE-2022-43685** | https://ckan.org/, https://ckan.org/blog/get-latest-patch-releases-your-ckan-site-october-2022 | A-OKF-CKAN-121222/482 |
| **Vendor: onion_project** | | | | | |
| **Product: onion** | | | | | |
| Affected Version(s): * Up to (excluding) 2022-09-05 | | | | | |
| Improper Resource Shutdown or Release | 19-Nov-2022 | 8.2 | A vulnerability was found in davidmoreno onion. It has been rated as problematic. Affected by this issue is the function onion_response_flush of the file src/onion/response.c of the component Log Handler. The manipulation leads to allocation of resources. The name of the patch is de8ea938342b36c28024fd8393ebc27b8442a161. It is recommended to apply a patch to fix this issue. The | https://github.com/davidmoreno/onion/commit/de8ea938342b36c28024fd8393ebc27b8442a161, https://github.com/davidmoreno/onion/pull/308 | A-ONI-ONIO-121222/483 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | identifier of this vulnerability is VDB-214028.<br>**CVE ID : CVE-2022-4066** |  |  |
| **Vendor: online-shopping-system-advanced_project** |  |  |  |  |  |
| **Product: online-shopping-system-advanced** |  |  |  |  |  |
| Affected Version(s): 1.0 |  |  |  |  |  |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 29-Nov-2022 | 9.8 | Online-shopping-system-advanced 1.0 was discovered to contain a SQL injection vulnerability via the p parameter at /shopping/product.php.<br>**CVE ID : CVE-2022-42109** | N/A | A-ONL-ONLI-121222/484 |
| **Vendor: online_diagnostic_lab_management_system_project** |  |  |  |  |  |
| **Product: online_diagnostic_lab_management_system** |  |  |  |  |  |
| Affected Version(s): 1.0 |  |  |  |  |  |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Nov-2022 | 9.8 | Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter at /diagnostic/login.php.<br>**CVE ID : CVE-2022-43135** | N/A | A-ONL-ONLI-121222/485 |
| Improper Neutralization of Special Elements used in an SQL Command | 17-Nov-2022 | 7.2 | Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tests/view_test.php. | N/A | A-ONL-ONLI-121222/486 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | **CVE ID : CVE-2022-43162** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 7.2 | Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /clients/view_client.php.<br>**CVE ID : CVE-2022-43163** | N/A | A-ONL-ONLI-121222/487 |
| **Vendor: online_leave_management_system_project** | | | | | |
| **Product: online_leave_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 7.2 | Online Leave Management System v1.0 was discovered to contain a SQL injection vulnerability via the component /admin/?page=user/manage_user&id=.<br>**CVE ID : CVE-2022-43179** | N/A | A-ONL-ONLI-121222/488 |
| **Vendor: online_tours_\&_travels_management_system_project** | | | | | |
| **Product: online_tours_\&_travels_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Unrestricted Upload of File with Dangerous Type | 28-Nov-2022 | 9.8 | Online Tours & Travels Management System v1.0 contains an arbitrary file upload vulnerability via /tour/admin/file.php.<br>**CVE ID : CVE-2022-44401** | N/A | A-ONL-ONLI-121222/489 |
| **Vendor: opcfoundation** | | | | | |
| **Product: local_discovery_server** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (excluding) 1.04.405.479 | | | | | |
| Incorrect Permission Assignment for Critical Resource | 17-Nov-2022 | 7.8 | OPC Foundation Local Discovery Server (LDS) through 1.04.403.478 uses a hard-coded file path to a configuration file. This allows a normal user to create a malicious file that is loaded by LDS (running as a high-privilege user).<br>**CVE ID : CVE-2022-44725** | https://opcfoundation.org/developer-tools/samples-and-tools-unified-architecture/local-discovery-server-lds/, https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2022-44725.pdf | A-OPC-LOCA-121222/490 |
| **Vendor: openjsf** | | | | | |
| **Product: express** | | | | | |
| Affected Version(s): * Up to (excluding) 4.17.3 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as | https://github.com/expressjs/express/releases/tag/4.17.3, https://github.com/ljharb/qs/pull/428 | A-OPE-EXPR-121222/491 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | | |
| **Vendor: orchardcore** | | | | | |
| **Product: orchard_cms** | | | | | |
| Affected Version(s): 1.10.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 9 | Orchardproject Orchard CMS 1.10.3 is vulnerable to Cross Site Scripting (XSS). When a low privileged user such as an author or publisher, injects a crafted html and javascript payload in a blog post, leading to full admin account takeover or privilege escalation when the malicious blog post is loaded in the victim's browser.<br>**CVE ID : CVE-2022-37720** | N/A | A-ORC-ORCH-121222/492 |
| **Vendor: oxilab** | | | | | |
| **Product: accordions** | | | | | |
| Affected Version(s): * Up to (excluding) 2.1.0 | | | | | |
| Improper Neutralization of | 18-Nov-2022 | 4.8 | Multiple Auth. (admin+) Stored Cross-Site Scripting | https://wordpress.org/plugins/accordio | A-OXI-ACCO-121222/493 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input During Web Page Generation ('Cross-site Scripting') | | | (XSS) vulnerabilities in Accordions plugin <= 2.0.3 on WordPress via &addons-style-name and &accordions_or_faqs_license_key.<br>**CVE ID : CVE-2022-45082** | ns-or-faqs/#developers, https://patchstack.com/database/vulnerability/accordions-or-faqs/wordpress-accordions-plugin-2-0-3-multiple-auth-stored-cross-site-scripting-xss-vulnerabilities?_s_id=cve | |
| **Product: image_hover_effects_ultimate** | | | | | |
| Affected Version(s): * Up to (including) 9.7.1 | | | | | |
| Improper Privilege Management | 18-Nov-2022 | 7.2 | Auth. WordPress Options Change vulnerability in Image Hover Effects Ultimate plugin <= 9.7.1 on WordPress.<br>**CVE ID : CVE-2022-42459** | https://patchstack.com/database/vulnerability/image-hover-effects-ultimate/wordpress-image-hover-effects-ultimate-plugin-9-7-1-auth-wordpress-options-change-vulnerability?_s_id=cve, https://wordpress.org/plugins/image-hover-effects-ultimate/ | A-OXI-IMAG-121222/494 |
| **Vendor: Parallels** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: remote_application_server** | | | | | |
| Affected Version(s): 18.0 | | | | | |
| Improper Encoding or Escaping of Output | 23-Nov-2022 | 8.1 | The Web Client of Parallels Remote Application Server v18.0 is vulnerable to Host Header Injection attacks. This vulnerability allows attackers to execute arbitrary commands via a crafted payload injected into the Host header.<br>**CVE ID : CVE-2022-40870** | N/A | A-PAR-REMO-121222/495 |
| **Vendor: password_storage_application_project** | | | | | |
| **Product: password_storage_application** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 6.1 | A cross-site scripting (XSS) vulnerability in the add-fee.php component of Password Storage Application v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter.<br>**CVE ID : CVE-2022-43142** | N/A | A-PAS-PASS-121222/496 |
| Improper Neutralization of Input During Web Page Generation | 21-Nov-2022 | 5.4 | Sourcecodester Password Storage Application in PHP/OOP and MySQL 1.0 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities | N/A | A-PAS-PASS-121222/497 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | via the Name, Username, Description and Site Feature parameters.<br>**CVE ID : CVE-2022-43117** | | |
| **Vendor: pencidesign** | | | | | |
| **Product: soledad** | | | | | |
| Affected Version(s): * Up to (excluding) 8.2.6 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Nov-2022 | 5.4 | Auth. (subscriber+) Cross-Site Scripting (XSS) vulnerability in Soledad premium theme <= 8.2.5 on WordPress.<br>**CVE ID : CVE-2022-41788** | https://themeforest.net/item/soledad-multiconcept-blogmagazine-wp-theme/12945398, https://patchstack.com/database/vulnerability/soledad/wordpress-soledad-premium-theme-8-2-5-auth-cross-site-scripting-xss-vulnerability?_s_id=cve | A-PEN-SOLE-121222/498 |
| **Vendor: permalink_manager_lite_project** | | | | | |
| **Product: permalink_manager_lite** | | | | | |
| Affected Version(s): * Up to (excluding) 2.2.20.1 | | | | | |
| N/A | 18-Nov-2022 | 9.8 | Broken Access Control vulnerability in Permalink Manager Lite plugin <= 2.2.20 on WordPress.<br>**CVE ID : CVE-2022-41781** | https://patchstack.com/database/vulnerability/permalink-manager/wordpress-permalink- | A-PER-PERM-121222/499 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | manager-lite-plugin-2-2-20-broken-access-control-vulnerability?_s_id=cve | |
| Affected Version(s): * Up to (excluding) 2.2.20.2 | | | | | |
| Cross-Site Request Forgery (CSRF) | 16-Nov-2022 | 4.3 | The Permalink Manager Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.2.20.1. This is due to missing or incorrect nonce validation on the extra_actions function. This makes it possible for unauthenticated attackers to change plugin settings including permalinks and site maps, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.<br>**CVE ID : CVE-2022-4021** | https://plugins.trac.wordpress.org/changeset/2818142#file34 | A-PER-PERM-121222/500 |
| **Vendor: phpgurukul_blood_donor_management_system_project** | | | | | |
| **Product: phpgurukul_blood_donor_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Exposure of Resource to Wrong Sphere | 25-Nov-2022 | 8.1 | PHPGurukul Blood Donor Management System 1.0 does not properly restrict access to admin/dashboard.php | N/A | A-PHP-PHPG-121222/501 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | , which allows attackers to access all data of users, delete the users, add and manage Blood Group, and Submit Report.<br>**CVE ID : CVE-2022-38813** | | |
| **Vendor: Postgresql** | | | | | |
| **Product: postgresql_jdbc_driver** | | | | | |
| Affected Version(s): 42.5.0 | | | | | |
| N/A | 23-Nov-2022 | 5.5 | pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that | https://github.com/pgjdbc/pgjdbc/commit/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5, https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-562r-vg33-8x8h | A-POS-POST-121222/502 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.<br>**CVE ID : CVE-2022-41946** | | |
| Affected Version(s): From (including) 42.2.0 Up to (excluding) 42.2.27 | | | | | |
| N/A | 23-Nov-2022 | 5.5 | pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, | https://github.com/pgjdbc/pgjdbc/commit/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5, https://github.com/pgjdbc/pgjdbc/security/advisories | A-POS-POST-121222/503 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable | /GHSA-562r-vg33-8x8h |  |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to a directory that is exclusively owned by the executing user will mitigate this vulnerability.<br>**CVE ID : CVE-2022-41946** | | |
| Affected Version(s): From (including) 42.3.0 Up to (excluding) 42.3.8 | | | | | |
| N/A | 23-Nov-2022 | 5.5 | pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents | https://github.com/pgjdbc/pgjdbc/commit/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5, https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-562r-vg33-8x8h | A-POS-POST-121222/504 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.<br>**CVE ID : CVE-2022-41946** | | |
| Affected Version(s): From (including) 42.4.0 Up to (excluding) 42.4.3 | | | | | |
| N/A | 23-Nov-2022 | 5.5 | pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This | https://github.com/pgjdbc/pgjdbc/commit/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5, https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-562r-vg33-8x8h | A-POS-POST-121222/505 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will |  |  |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | mitigate this vulnerability.<br>**CVE ID : CVE-2022-41946** | | |
| **Vendor: purchase_order_management_system_project** | | | | | |
| **Product: purchase_order_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Unrestricted Upload of File with Dangerous Type | 28-Nov-2022 | 9.8 | Purchase Order Management System v1.0 contains a file upload vulnerability via /purchase_order/admin/?page=system_info.<br>**CVE ID : CVE-2022-44400** | N/A | A-PUR-PURC-121222/506 |
| **Vendor: pyrocms** | | | | | |
| **Product: pyrocms** | | | | | |
| Affected Version(s): 3.9 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 9 | PyroCMS 3.9 is vulnerable to a stored Cross Site Scripting (XSS_ when a low privileged user such as an author, injects a crafted html and javascript payload in a blog post, leading to full admin account takeover or privilege escalation.<br>**CVE ID : CVE-2022-37721** | N/A | A-PYR-PYRO-121222/507 |
| **Vendor: qpress_project** | | | | | |
| **Product: qpress** | | | | | |
| Affected Version(s): * Up to (excluding) 11.3 | | | | | |
| Improper Limitation of a | 23-Nov-2022 | 5.3 | qpress before PierreLvx/qpress 20220819 and before | https://github.com/EvgeniyPatlan/qpres | A-QPR-QPRE-121222/508 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pathname to a Restricted Directory ('Path Traversal') | | | version 11.3, as used in Percona XtraBackup and other products, allows directory traversal via ../ in a .qp file.<br>**CVE ID : CVE-2022-45866** | s/commit/ddb312090ebd5794e81bc6fb1dfb4e79eda48761, https://github.com/PierreLvx/qpress/compare/20170415...20220819 | |
| **Vendor: qs_project** | | | | | |
| **Product: qs** | | | | | |
| Affected Version(s): * Up to (excluding) 6.2.4 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release | https://github.com/expressjs/express/releases/tag/4.17.3, https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/509 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | | |
| Affected Version(s): 6.4.0 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | https://github.com/expressjs/express/releases/tag/4.17.3, https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/510 |
| Affected Version(s): 6.6.0 | | | | | |
| Improperly Controlled Modification of Object | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows | https://github.com/expressjs/express/releases/tag/4. | A-QS_-QS-121222/511 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Prototype Attributes ('Prototype Pollution') | | | attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | 17.3, https://github.com/ljharb/qs/pull/428 | |
| Affected Version(s): From (including) 6.10.0 Up to (excluding) 6.10.3 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack | https://github.com/expressjs/express/releases/tag/4.17.3, https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/512 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | | |
| Affected Version(s): From (including) 6.3.0 Up to (excluding) 6.3.3 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and | https://github.com/expressjs/express/releases/tag/4.17.3, https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/513 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | | |
| Affected Version(s): From (including) 6.5.0 Up to (excluding) 6.5.3 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | https://github.com/expressjs/express/releases/tag/4.17.3,<br>https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/514 |
| Affected Version(s): From (including) 6.7.0 Up to (excluding) 6.7.3 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an _ proto_ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[_proto_]=b&a[_proto_]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | https://github.com/expressjs/express/releases/tag/4.17.3,<br>https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/515 |
| Affected Version(s): From (including) 6.8.0 Up to (excluding) 6.8.3 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an _ proto_ key can be used. In many typical Express | https://github.com/expressjs/express/releases/tag/4.17.3,<br>https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/516 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | | |
| Affected Version(s): From (including) 6.9.0 Up to (excluding) 6.9.7 | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 26-Nov-2022 | 7.5 | qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100 | https://github.com/expressjs/express/releases/tag/4.17.3, https://github.com/ljharb/qs/pull/428 | A-QS_-QS-121222/517 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).<br>**CVE ID : CVE-2022-24999** | | |
| **Vendor: rconfig** | | | | | |
| **Product: rconfig** | | | | | |
| Affected Version(s): 3.9.6 | | | | | |
| Unrestricted Upload of File with Dangerous Type | 17-Nov-2022 | 8.8 | An arbitrary file upload vulnerability in rconfig v3.9.6 allows attackers to execute arbitrary code via a crafted PHP file.<br>**CVE ID : CVE-2022-44384** | N/A | A-RCO-RCON-121222/518 |
| **Vendor: recaptcha_project** | | | | | |
| **Product: recaptcha** | | | | | |
| Affected Version(s): * Up to (including) 1.6 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The reCAPTCHA WordPress plugin through 1.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for | N/A | A-REC-RECA-121222/519 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | example in multisite setup).<br>**CVE ID : CVE-2022-3831** | | |
| **Vendor: record_management_system_project** | | | | | |
| **Product: record_management_system** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 23-Nov-2022 | 5.4 | An access control issue in /Admin/dashboard.php of Record Management System using CodeIgniter v1.0 allows attackers to access and modify user data.<br>**CVE ID : CVE-2022-41446** | N/A | A-REC-RECO-121222/520 |
| **Vendor: Redhat** | | | | | |
| **Product: build_of_quarkus** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 22-Nov-2022 | 9.8 | A vulnerability was found in quarkus. This security flaw happens in Dev UI Config Editor which is vulnerable to drive-by localhost attacks leading to remote code execution.<br>**CVE ID : CVE-2022-4116** | https://access.redhat.com/security/cve/CVE-2022-4116 | A-RED-BUIL-121222/521 |
| **Vendor: redlion** | | | | | |
| **Product: crimson** | | | | | |
| Affected Version(s): * Up to (excluding) 3.0 | | | | | |
| Improper Limitation of a Pathname | 17-Nov-2022 | 5.3 | Red Lion Controls Crimson 3.0 versions 707.000 and prior, Crimson 3.1 versions | N/A | A-RED-CRIM-121222/522 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| to a Restricted Directory ('Path Traversal') | | | 3126.001 and prior, and Crimson 3.2 versions 3.2.0044.0 and prior are vulnerable to path traversal. When attempting to open a file using a specific path, the user's password hash is sent to an arbitrary host. This could allow an attacker to obtain user credential hashes.<br>**CVE ID : CVE-2022-3090** | | |
| Affected Version(s): 3.0 | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Nov-2022 | 5.3 | Red Lion Controls Crimson 3.0 versions 707.000 and prior, Crimson 3.1 versions 3126.001 and prior, and Crimson 3.2 versions 3.2.0044.0 and prior are vulnerable to path traversal. When attempting to open a file using a specific path, the user's password hash is sent to an arbitrary host. This could allow an attacker to obtain user credential hashes.<br>**CVE ID : CVE-2022-3090** | N/A | A-RED-CRIM-121222/523 |
| Affected Version(s): 3.1 | | | | | |
| Improper Limitation of a Pathname | 17-Nov-2022 | 5.3 | Red Lion Controls Crimson 3.0 versions 707.000 and prior, Crimson 3.1 versions | N/A | A-RED-CRIM-121222/524 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| to a Restricted Directory ('Path Traversal') | | | 3126.001 and prior, and Crimson 3.2 versions 3.2.0044.0 and prior are vulnerable to path traversal. When attempting to open a file using a specific path, the user's password hash is sent to an arbitrary host. This could allow an attacker to obtain user credential hashes.<br>**CVE ID : CVE-2022-3090** | | |
| Affected Version(s): 3.2 | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Nov-2022 | 5.3 | Red Lion Controls Crimson 3.0 versions 707.000 and prior, Crimson 3.1 versions 3126.001 and prior, and Crimson 3.2 versions 3.2.0044.0 and prior are vulnerable to path traversal. When attempting to open a file using a specific path, the user's password hash is sent to an arbitrary host. This could allow an attacker to obtain user credential hashes.<br>**CVE ID : CVE-2022-3090** | N/A | A-RED-CRIM-121222/525 |
| **Vendor: richplugins** | | | | | |
| **Product: plugin_for_google_reviews** | | | | | |
| Affected Version(s): * Up to (excluding) 2.2.3 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 18-Nov-2022 | 4.3 | Auth. (subscriber+) Broken Access Control vulnerability in Plugin for Google Reviews plugin <= 2.2.2 on WordPress.<br>**CVE ID : CVE-2022-45369** | https://patchstack.com/database/vulnerability/widget-google-reviews/wordpress-plugin-for-google-reviews-plugin-2-2-2-auth-broken-access-control-vulnerability?_s_id=cve | A-RIC-PLUG-121222/526 |
| **Vendor: salat_times_project** | | | | | |
| **Product: salat_times** | | | | | |
| Affected Version(s): * Up to (excluding) 3.2.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Salat Times WordPress plugin before 3.2.2 does not sanitize and escapes its settings, allowing high-privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.<br>**CVE ID : CVE-2022-2983** | N/A | A-SAL-SALA-121222/527 |
| **Vendor: sandhillsdev** | | | | | |
| **Product: easy_digital_downloads** | | | | | |
| Affected Version(s): * Up to (excluding) 3.1.0.2 | | | | | |
| Improper Neutralization of Formula Elements | 21-Nov-2022 | 9.8 | The Easy Digital Downloads WordPress plugin before 3.1.0.2 does not validate data when its | https://wpscan.com/vulnerability/16e2d970-19d0-42d1-8fb1- | A-SAN-EASY-121222/528 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| in a CSV File | | | output in a CSV file, which could lead to CSV injection.<br>**CVE ID : CVE-2022-3600** | e7cb14ace1d0 | |
| **Vendor: sanitization_management_system_project** | | | | | |
| **Product: sanitization_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Nov-2022 | 7.2 | Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/?page=user/manage_user&id=.<br>**CVE ID : CVE-2022-44278** | N/A | A-SAN-SANI-121222/529 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 6.1 | A cross-site scripting (XSS) vulnerability in Sanitization Management System v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter at /php-sms/classes/Login.php.<br>**CVE ID : CVE-2022-45214** | N/A | A-SAN-SANI-121222/530 |
| **Vendor: sankhya** | | | | | |
| **Product: sankhya_om** | | | | | |
| Affected Version(s): * Up to (excluding) 4.11b81 | | | | | |
| Improper Neutralization of Input | 22-Nov-2022 | 9 | ERP Sankhya before v4.11b81 was discovered to contain a cross-site scripting | N/A | A-SAN-SANK-121222/531 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | (XSS) vulnerability via the component Caixa de Entrada.<br>**CVE ID : CVE-2022-42989** | | |
| **Vendor: school_management_system_project** | | | | | |
| **Product: school_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 28-Nov-2022 | 9.8 | SQL injection in School Management System 1.0 allows remote attackers to modify or delete data, causing persistent changes to the application's content or behavior by using malicious SQL queries.<br>**CVE ID : CVE-2022-36193** | N/A | A-SCH-SCHO-121222/532 |
| **Vendor: scratch-wiki** | | | | | |
| **Product: scratch_login** | | | | | |
| Affected Version(s): * Up to (including) 1.1 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 4.8 | The ScratchLogin extension through 1.1 for MediaWiki does not escape verification failure messages, which allows users with administrator privileges to perform cross-site scripting (XSS).<br>**CVE ID : CVE-2022-42985** | https://github.com/InternationalScratchWiki/mediawiki-scratch-login/blob/4d2c1229b558b9cd685961274f20b621d114f4db/ScratchLogin.common.php#L104,<br>https://github.com/InternationalScratchWiki/mediawi | A-SCR-SCRA-121222/533 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | ki-scratch-login/pull/22 | |
| **Vendor: seacms** | | | | | |
| **Product: seacms** | | | | | |
| Affected Version(s): * Up to (excluding) 12.6 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Nov-2022 | 9.8 | SeaCms before v12.6 was discovered to contain a SQL injection vulnerability via the component /js/player/dmplayer/dmku/index.php.<br>**CVE ID : CVE-2022-43256** | N/A | A-SEA-SEAC-121222/534 |
| **Vendor: showing_url_in_qr_code_project** | | | | | |
| **Product: showing_url_in_qr_code** | | | | | |
| Affected Version(s): 0.0.1 | | | | | |
| Cross-Site Request Forgery (CSRF) | 28-Nov-2022 | 6.1 | The Showing URL in QR Code WordPress plugin through 0.0.1 does not have CSRF check when updating its settings, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin or editor add Stored XSS payloads via a CSRF attack<br>**CVE ID : CVE-2022-3847** | N/A | A-SHO-SHOW-121222/535 |
| **Vendor: Siemens** | | | | | |
| **Product: syngo_dynamics_cardiovascular_imaging_and_information_system** | | | | | |
| Affected Version(s): * Up to (excluding) va40g_hf01 | | | | | |
| Externally Controlled | 17-Nov-2022 | 7.5 | A vulnerability has been identified in | https://www.siemens- | A-SIE-SYNG-121222/536 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Reference to a Resource in Another Sphere | | | syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper read access control that could allow files to be retrieved from any folder accessible to the account assigned to the website's application pool.<br>**CVE ID : CVE-2022-42732** | healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 | |
| Externally Controlled Reference to a Resource in Another Sphere | 17-Nov-2022 | 7.5 | A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper read access control that could allow files to be retrieved from any folder accessible to the account assigned to the website's application pool.<br>**CVE ID : CVE-2022-42733** | https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 | A-SIE-SYNG-121222/537 |
| Externally Controlled Reference to a Resource | 17-Nov-2022 | 7.5 | A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web | https://www.siemens-healthineers.com/en-us/support-documentation/cybersecuri | A-SIE-SYNG-121222/538 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| in Another Sphere | | | service using an operation with improper write access control that could allow to write data in any folder accessible to the account assigned to the website's application pool.<br>**CVE ID : CVE-2022-42734** | ty/shsa-741697 | |
| Externally Controlled Reference to a Resource in Another Sphere | 17-Nov-2022 | 7.5 | A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow to write data in any folder accessible to the account assigned to the website's application pool.<br>**CVE ID : CVE-2022-42891** | https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 | A-SIE-SYNG-121222/539 |
| Externally Controlled Reference to a Resource in Another Sphere | 17-Nov-2022 | 7.5 | A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow to write data in | https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 | A-SIE-SYNG-121222/540 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | any folder accessible to the account assigned to the website’s application pool.<br>**CVE ID : CVE-2022-42893** | | |
| Server-Side Request Forgery (SSRF) | 17-Nov-2022 | 7.5 | A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). An unauthenticated Server-Side Request Forgery (SSRF) vulnerability was identified in one of the web services exposed on the syngo Dynamics application that could allow for the leaking of NTLM credentials as well as local service enumeration.<br>**CVE ID : CVE-2022-42894** | https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 | A-SIE-SYNG-121222/541 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Nov-2022 | 5.3 | A vulnerability has been identified in syngo Dynamics (All versions < VA40G HF01). syngo Dynamics application server hosts a web service using an operation with improper write access control that could allow directory listing in any folder accessible to the account assigned to | https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-741697 | A-SIE-SYNG-121222/542 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the website's application pool.<br>**CVE ID : CVE-2022-42892** | | |
| **Vendor: silabs** | | | | | |
| **Product: gecko_software_development_kit** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 18-Nov-2022 | 6.5 | A malformed packet containing an invalid destination address, causes a stack overflow in the Ember ZNet stack. This causes an assert which leads to a reset, immediately clearing the error.<br>**CVE ID : CVE-2022-24939** | https://siliconlabs.lightning.force.com/sfc/servlet.shepherd/document/download/0698Y00000IWDCwQAP?operationContext=S1 | A-SIL-GECK-121222/543 |
| **Product: zigbee_emberznet** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 18-Nov-2022 | 6.5 | A malformed packet containing an invalid destination address, causes a stack overflow in the Ember ZNet stack. This causes an assert which leads to a reset, immediately clearing the error.<br>**CVE ID : CVE-2022-24939** | https://siliconlabs.lightning.force.com/sfc/servlet.shepherd/document/download/0698Y00000IWDCwQAP?operationContext=S1 | A-SIL-ZIGB-121222/544 |
| **Vendor: Silverstripe** | | | | | |
| **Product: assets** | | | | | |
| Affected Version(s): From (including) 1.0.0 Up to (including) 1.11.0 | | | | | |
| Improper Neutralization of | 23-Nov-2022 | 5.4 | Silverstripe silverstripe/framework through 4.11.0, | https://www.silverstripe.org/download/s | A-SIL-ASSE-121222/545 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input During Web Page Generation ('Cross-site Scripting') | | | silverstripe/assets through 1.11.0, and silverstripe/asset-admin through 1.11.0 allow XSS.<br>**CVE ID : CVE-2022-38724** | ecurity-releases/, https://www.silverstripe.org/blog/tag/release, https://forum.silverstripe.org/c/releases, https://www.silverstripe.org/download/security-releases/CVE-2022-38724 | |
| **Product: asset_admin** | | | | | |
| Affected Version(s): * Up to (including) 1.11.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | Silverstripe silverstripe/framework through 4.11.0, silverstripe/assets through 1.11.0, and silverstripe/asset-admin through 1.11.0 allow XSS.<br>**CVE ID : CVE-2022-38724** | https://www.silverstripe.org/download/security-releases/, https://www.silverstripe.org/blog/tag/release, https://forum.silverstripe.org/c/releases, https://www.silverstripe.org/download/security-releases/CVE-2022-38724 | A-SIL-ASSE-121222/546 |
| **Product: framework** | | | | | |
| Affected Version(s): * Up to (excluding) 4.11.13 | | | | | |
| Improper Neutralization of Input During | 22-Nov-2022 | 6.1 | Silverstripe silverstripe/framework through 4.11 is vulnerable to XSS by carefully crafting a | https://www.silverstripe.org/download/security-releases/, | A-SIL-FRAM-121222/547 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | return URL on a /dev/build or /Security/login request.<br>**CVE ID : CVE-2022-38462** | https://www.silverstripe.org/blog/tag/release, https://forum.silverstripe.org/c/releases | |
| Affected Version(s): * Up to (including) 4.11.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 21-Nov-2022 | 8.8 | Silverstripe silverstripe/framework through 4.11 allows SQL Injection.<br>**CVE ID : CVE-2022-38148** | https://www.silverstripe.org/download/security-releases/, https://www.silverstripe.org/download/security-releases/CVE-2022-38148, https://www.silverstripe.org/blog/tag/release, https://forum.silverstripe.org/c/releases | A-SIL-FRAM-121222/548 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 5.4 | Silverstripe silverstripe/framework through 4.11 allows XSS (issue 2 of 3).<br>**CVE ID : CVE-2022-38146** | https://www.silverstripe.org/download/security-releases/CVE-2022-38146, https://www.silverstripe.org/download/security-releases/, https://www.silverstripe.org/blog/tag/release, https://forum | A-SIL-FRAM-121222/549 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | .silverstripe.org/c/releases | |
| Affected Version(s): From (including) 3.0.0 Up to (including) 3.7.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 6.1 | Silverstripe silverstripe/framework through 4.11 is vulnerable to XSS by carefully crafting a return URL on a /dev/build or /Security/login request.<br>**CVE ID : CVE-2022-38462** | https://www.silverstripe.org/download/security-releases/, https://www.silverstripe.org/blog/tag/release, https://forum.silverstripe.org/c/releases | A-SIL-FRAM-121222/550 |
| Affected Version(s): From (including) 3.0.0 Up to (including) 4.11 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | Silverstripe silverstripe/framework through 4.11 allows XSS (issue 1 of 2) via JavaScript payload to the href attribute of a link by splitting a javascript URL with white space characters.<br>**CVE ID : CVE-2022-37429** | https://www.silverstripe.org/download/security-releases/, https://www.silverstripe.org/download/security-releases/CVE-2022-37429, https://www.silverstripe.org/blog/tag/release, https://forum.silverstripe.org/c/releases | A-SIL-FRAM-121222/551 |
| Affected Version(s): From (including) 4.0.0 Up to (including) 4.11.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation | 23-Nov-2022 | 5.4 | Silverstripe silverstripe/framework through 4.11.0, silverstripe/assets through 1.11.0, and silverstripe/asset- | https://www.silverstripe.org/download/security-releases/, https://www.silverstripe.or | A-SIL-FRAM-121222/552 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | admin through 1.11.0 allow XSS.<br>**CVE ID : CVE-2022-38724** | g/blog/tag/release, https://forum.silverstripe.org/c/releases, https://www.silverstripe.org/download/security-releases/CVE-2022-38724 | |
| **Vendor: simple_history_project** | | | | | |
| **Product: simple_history** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 16-Nov-2022 | 9.8 | A vulnerability was found in Simple History Plugin. It has been rated as critical. This issue affects some unknown processing of the component Header Handler. The manipulation of the argument X-Forwarded-For leads to improper output neutralization for logs. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213785 was assigned to this vulnerability.<br>**CVE ID : CVE-2022-4011** | N/A | A-SIM-SIMP-121222/553 |
| **Vendor: socket** | | | | | |
| **Product: engine.io** | | | | | |
| Affected Version(s): * Up to (excluding) 3.6.1 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncaught Exception | 22-Nov-2022 | 6.5 | Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the engine.io package, including those who uses depending packages like socket.io. There is no known workaround except upgrading to a safe version. There are patches for this issue released in versions 3.6.1 and 6.2.1.<br>**CVE ID : CVE-2022-41940** | https://github.com/socketio/engine.io/commit/83c4071af871fc188298d7d591e95670bf9f9085 , https://github.com/socketio/engine.io/commit/425e833ab13373edf1dd5a0706f07100db14e3c6, https://github.com/socketio/engine.io/security/advisories/GHSA-r7qp-cfhv-p84w | A-SOC-ENGI-121222/554 |
| Affected Version(s): From (including) 4.0.0 Up to (excluding) 6.2.1 | | | | | |
| Uncaught Exception | 22-Nov-2022 | 6.5 | Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users | https://github.com/socketio/engine.io/commit/83c4071af871fc188298d7d591e95670bf9f9085 , https://github.com/socketio/engine.io/commit/425e833ab13373edf1dd5a0706f0 | A-SOC-ENGI-121222/555 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of the engine.io package, including those who uses depending packages like socket.io. There is no known workaround except upgrading to a safe version. There are patches for this issue released in versions 3.6.1 and 6.2.1.<br>**CVE ID : CVE-2022-41940** | 7100db14e3c6, https://github.com/socketio/engine.io/security/advisories/GHSA-r7qp-cfhv-p84w | |
| **Vendor: Solarwinds** | | | | | |
| **Product: security_event_manager** | | | | | |
| Affected Version(s): * Up to (excluding) 2022.2 | | | | | |
| Interpretation Conflict | 23-Nov-2022 | 5.3 | Insecure method vulnerability in which allowed HTTP methods are disclosed. E.g., OPTIONS, DELETE, TRACE, and PUT<br>**CVE ID : CVE-2022-38115** | https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38115, https://documentation.solarwinds.com/en/success_center/sem/content/release_notes/sem_2022-4_release_notes.htm | A-SOL-SECU-121222/556 |
| Affected Version(s): * Up to (excluding) 2022.4 | | | | | |
| N/A | 23-Nov-2022 | 6.1 | This vulnerability occurs when a web server fails to correctly process the Content-Length of POST requests. This | https://documentation.solarwinds.com/en/success_center/sem/content/release_ | A-SOL-SECU-121222/557 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | can lead to HTTP request smuggling or XSS.<br>**CVE ID : CVE-2022-38114** | notes/sem_2022-4_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38114 | |
| Affected Version(s): 2022.4 | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 23-Nov-2022 | 5.3 | This vulnerability discloses build and services versions in the server response header.<br>**CVE ID : CVE-2022-38113** | https://documentation.solarwinds.com/en/success_center/sem/content/release_notes/sem_2022-4_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38113 | A-SOL-SECU-121222/558 |
| **Vendor: Sophos** | | | | | |
| **Product: mobile** | | | | | |
| Affected Version(s): From (including) 5.0.0 Up to (excluding) 9.7.5 | | | | | |
| Improper Restriction of XML External Entity Reference | 16-Nov-2022 | 9.8 | An XML External Entity (XEE) vulnerability allows server-side request forgery (SSRF) and potential code execution in Sophos Mobile managed on- | https://www.sophos.com/en-us/security-advisories/sophos-sa-20221116-smc-xee | A-SOP-MOBI-121222/559 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | premises between versions 5.0.0 and 9.7.4.<br>**CVE ID : CVE-2022-3980** | | |
| **Vendor: sourcegraph** | | | | | |
| **Product: sourcegraph** | | | | | |
| Affected Version(s): * Up to (excluding) 4.1.0 | | | | | |
| Improper Input Validation | 22-Nov-2022 | 7.8 | Sourcegraph is a code intelligence platform. In versions prior to 4.1.0 a command Injection vulnerability existed in the gitserver service, present in all Sourcegraph deployments. This vulnerability was caused by a lack of input validation on the host parameter of the `/list-gitolite` endpoint. It was possible to send a crafted request to gitserver that would execute commands inside the container. Successful exploitation requires the ability to send local requests to gitserver. The issue is patched in version 4.1.0.<br>**CVE ID : CVE-2022-41942** | https://github.com/sourcegraph/sourcegraph/security/advisories/GHSA-pfm3-23mh-6xjp, https://github.com/sourcegraph/sourcegraph/pull/42553 | A-SOU-SOUR-121222/560 |
| Incorrect Default | 22-Nov-2022 | 7.2 | sourcegraph is a code intelligence platform. As a site admin it was possible to execute | https://github.com/sourcegraph/sourcegraph/pull/4 | A-SOU-SOUR-121222/561 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Permissions | | | arbitrary commands on Gitserver when the experimental `customGitFetch` feature was enabled. This experimental feature has now been disabled by default. This issue has been patched in version 4.1.0.<br>**CVE ID : CVE-2022-41943** | 2704, https://github.com/sourcegraph/sourcegraph/security/advisories/GHSA-4qhq-4x4h-fxm8 | |
| **Vendor: spatie** | | | | | |
| **Product: browsershot** | | | | | |
| Affected Version(s): 3.57.2 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 6.1 | Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate that the HTML content passed to the Browsershot::html method does not contain URL's that use the file:// protocol.<br>**CVE ID : CVE-2022-43983** | N/A | A-SPA-BROW-121222/562 |
| Affected Version(s): 3.57.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation | 25-Nov-2022 | 6.1 | Browsershot version 3.57.3 allows an external attacker to remotely obtain arbitrary local files. This is possible because the | N/A | A-SPA-BROW-121222/563 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | application does not validate that the JS content imported from an external source passed to the Browsershot::html method does not contain URLs that use the file:// protocol.<br>**CVE ID : CVE-2022-43984** | | |
| **Vendor: sports_club_management_system_project** | | | | | |
| **Product: sports_club_management_system** | | | | | |
| Affected Version(s): 119 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Nov-2022 | 9.8 | A vulnerability, which was classified as critical, was found in Sports Club Management System 119. This affects an unknown part of the file admin/make_payments.php. The manipulation of the argument m_id/plan leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213789 was assigned to this vulnerability.<br>**CVE ID : CVE-2022-4015** | N/A | A-SPO-SPOR-121222/564 |
| **Vendor: stock_management_system_project** | | | | | |
| **Product: stock_management_system** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 24-Nov-2022 | 9.8 | A vulnerability was found in rickxy Stock Management System and classified as critical. Affected by this issue is some unknown functionality of the file /pages/processlogin.php. The manipulation of the argument user/password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-214322 is the identifier assigned to this vulnerability.<br>**CVE ID : CVE-2022-4088** | N/A | A-STO-STOC-121222/565 |
| Cross-Site Request Forgery (CSRF) | 24-Nov-2022 | 8.8 | A vulnerability was found in rickxy Stock Management System and classified as problematic. This issue affects some unknown processing of the file us_transac.php?action=add. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this | N/A | A-STO-STOC-121222/566 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability is VDB-214331.<br>**CVE ID : CVE-2022-4090** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 24-Nov-2022 | 5.4 | A vulnerability was found in rickxy Stock Management System. It has been declared as problematic. This vulnerability affects unknown code of the file /pages/processlogin.php. The manipulation of the argument user leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214324.<br>**CVE ID : CVE-2022-4089** | N/A | A-STO-STOC-121222/567 |
| **Vendor: storeapps** | | | | | |
| **Product: news_announcement_scroll** | | | | | |
| Affected Version(s): * Up to (including) 8.8.8 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 4.8 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in News Announcement Scroll plugin <= 8.8.8 on WordPress.<br>**CVE ID : CVE-2022-40694** | https://patchstack.com/database/vulnerability/news-announcement-scroll/wordpress-news-announcement-scroll-plugin-8-8-8-auth-stored-cross-site- | A-STO-NEWS-121222/568 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | scripting-xss-vulnerability?_s_id=cve | |
| **Vendor: student_attendance_management_system_project** | | | | | |
| **Product: student_attendance_management_system** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 7.2 | A vulnerability was found in Student Attendance Management System and classified as critical. This issue affects some unknown processing of the file /Admin/createClass.php. The manipulation of the argument Id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213845 was assigned to this vulnerability.<br>**CVE ID : CVE-2022-4052** | N/A | A-STU-STUD-121222/569 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 4.8 | A vulnerability was found in Student Attendance Management System. It has been classified as problematic. Affected is an unknown function of the file createClass.php. The manipulation of the argument className leads to cross site scripting. It is possible | N/A | A-STU-STUD-121222/570 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-213846 is the identifier assigned to this vulnerability.<br>**CVE ID : CVE-2022-4053** | | |
| **Vendor: super-xray_project** | | | | | |
| **Product: super-xray** | | | | | |
| Affected Version(s): 0.1 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 21-Nov-2022 | 9.8 | super-xray is a vulnerability scanner (xray) GUI launcher. In version 0.1-beta, the URL is not filtered and directly spliced ??into the command, resulting in a possible RCE vulnerability. Users should upgrade to super-xray 0.2-beta.<br>**CVE ID : CVE-2022-41945** | https://github.com/4ra1n/super-xray/security/advisories/GHSA-732j-763p-cvqg | A-SUP-SUPE-121222/571 |
| **Vendor: super_xray_project** | | | | | |
| **Product: super_xray** | | | | | |
| Affected Version(s): 0.2 | | | | | |
| Execution with Unnecessary Privileges | 22-Nov-2022 | 7.8 | super-xray is the GUI alternative for vulnerability scanning tool xray. In 0.2-beta, a privilege escalation vulnerability was discovered. This caused inaccurate default xray permissions. Note: this vulnerability only affects Linux and Mac OS systems. Users | https://github.com/4ra1n/super-xray/security/advisories/GHSA-2g28-xrw6-fq5f | A-SUP-SUPE-121222/572 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | should upgrade to super-xray 0.3-beta.<br>**CVE ID : CVE-2022-41950** | | |
| **Vendor: teacher_record_management_system_project** | | | | | |
| **Product: teacher_record_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in Record Management System using CodeIgniter 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Add Subject page.<br>**CVE ID : CVE-2022-41445** | N/A | A-TEA-TEAC-121222/573 |
| **Vendor: technitium** | | | | | |
| **Product: dns_server** | | | | | |
| Affected Version(s): * Up to (including) 8.0.2 | | | | | |
| Use of Incorrectly-Resolved Name or Reference | 21-Nov-2022 | 9.8 | An issue was discovered in Technitium DNS Server through 8.0.2 that allows variant V1 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS | N/A | A-TEC-DNS_-121222/574 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.<br>**CVE ID : CVE-2022-30257** |  |  |
| Use of Incorrectly-Resolved Name or Reference | 21-Nov-2022 | 9.8 | An issue was discovered in Technitium DNS Server through 8.0.2 that allows variant V2 of unintended domain name resolution. A revoked domain name can still be resolvable for a long time, including expired domains and taken-down malicious domains. The effects of an exploit would be widespread and highly impactful, because the exploitation conforms to de facto DNS specifications and operational practices, and overcomes current mitigation patches for "Ghost" domain names.<br>**CVE ID : CVE-2022-30258** | N/A | A-TEC-DNS_-121222/575 |
| **Vendor: testng_project** |  |  |  |  |  |
| **Product: testng** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Improper Limitation of a Pathname | 19-Nov-2022 | 7.8 | A vulnerability was found in cbeust testng. It has been declared as critical. Affected by | https://github.com/cbeust/testng/commit/9150736 | A-TES-TEST-121222/576 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| to a Restricted Directory ('Path Traversal') | | | this vulnerability is the function testngXmlExistsInJar of the file testng-core/src/main/java/org/testng/JarFileUtils.java of the component XML File Parser. The manipulation leads to path traversal. The attack can be launched remotely. The name of the patch is 9150736cd2c123a6a3b60e6193630859f9f0422b. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-214027.<br>**CVE ID : CVE-2022-4065** | cd2c123a6a3b60e6193630859f9f0422b, https://github.com/cbeust/testng/pull/2806 | |
| **Vendor: thematosoup** | | | | | |
| **Product: fancier_author_box** | | | | | |
| Affected Version(s): * Up to (including) 1.4 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Fancier Author Box by ThematoSoup WordPress plugin through 1.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for | N/A | A-THE-FANC-121222/577 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | example in multisite setup).<br>**CVE ID : CVE-2022-3833** | | |
| **Vendor: themeum** | | | | | |
| **Product: wp_page_builder** | | | | | |
| Affected Version(s): * Up to (excluding) 1.2.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Nov-2022 | 5.4 | Multiple Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerabilities in WP Page Builder plugin <= 1.2.6 on WordPress.<br>**CVE ID : CVE-2022-40963** | https://wordpress.org/plugins/wp-pagebuilder/, https://patchstack.com/database/vulnerability/wp-pagebuilder/wordpress-wp-page-builder-plugin-1-2-6-multiple-auth-stored-cross-site-scripting-xss-vulnerabilities?_s_id=cve | A-THE-WP_P-121222/578 |
| **Vendor: thriveweb** | | | | | |
| **Product: wooswipe_woocommerce_gallery** | | | | | |
| Affected Version(s): * Up to (including) 2.0.1 | | | | | |
| N/A | 17-Nov-2022 | 8.8 | Auth. (subscriber+) Broken Access Control vulnerability in WooSwipe WooCommerce Gallery plugin <= 2.0.1 on WordPress.<br>**CVE ID : CVE-2022-45066** | https://patchstack.com/database/vulnerability/wooswipe/wordpress-wooswipe-woocommerce-gallery-plugin-2-0-1-auth-broken-access- | A-THR-WOOS-121222/579 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | control-vulnerability?_s_id=cve | |
| **Vendor: Tipsandtricks-hq** | | | | | |
| **Product: all_in_one_wp_security_\&_firewall** | | | | | |
| Affected Version(s): * Up to (including) 5.1.0 | | | | | |
| Cross-Site Request Forgery (CSRF) | 22-Nov-2022 | 8.8 | Multiple Cross-Site Request Forgery vulnerabilities in All-In-One Security (AIOS) – Security and Firewall (WordPress plugin) <= 5.1.0 on WordPress.<br>**CVE ID : CVE-2022-44737** | N/A | A-TIP-ALL_-121222/580 |
| **Product: donations_via_paypal** | | | | | |
| Affected Version(s): * Up to (excluding) 1.9.9 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Donations via PayPal WordPress plugin before 1.9.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3822** | N/A | A-TIP-DONA-121222/581 |
| **Vendor: tooljet** | | | | | |
| **Product: tooljet** | | | | | |
| Affected Version(s): * Up to (excluding) 1.27.0 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncontrolled Resource Consumption | 22-Nov-2022 | 6.5 | Unrestricted file size limit can lead to DoS in tooljet/tooljet <1.27 by allowing a logged in attacker to upload profile pictures over 2MB.<br>**CVE ID : CVE-2022-4111** | https://github.com/tooljet/tooljet/commit/01cd3f0464747973ec329e9fb1ea12743d3235cc, https://huntr.dev/bounties/5596d072-66d2-4361-8cac-101c9c781c3d | A-TOO-TOOL-121222/582 |
| **Vendor: tribalsystems** | | | | | |
| **Product: zenario** | | | | | |
| Affected Version(s): 9.3.57186 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Nov-2022 | 5.4 | Zenario CMS 9.3.57186 is vulnerable to Cross Site Scripting (XSS) via the Nest library module.<br>**CVE ID : CVE-2022-44069** | N/A | A-TRI-ZENA-121222/583 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Nov-2022 | 5.4 | Zenario CMS 9.3.57186 is vulnerable to Cross Site Scripting (XSS) via News articles.<br>**CVE ID : CVE-2022-44070** | N/A | A-TRI-ZENA-121222/584 |
| Improper Neutralization of Input During Web Page Generation | 16-Nov-2022 | 5.4 | Zenario CMS 9.3.57186 is is vulnerable to Cross Site Scripting (XSS) via profile. | N/A | A-TRI-ZENA-121222/585 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | **CVE ID : CVE-2022-44071** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Nov-2022 | 5.4 | Zenario CMS 9.3.57186 is vulnerable to Cross Site Scripting (XSS) via svg,Users & Contacts.<br>**CVE ID : CVE-2022-44073** | N/A | A-TRI-ZENA-121222/586 |
| **Vendor: ujsoftware** | | | | | |
| **Product: owm_weather** | | | | | |
| Affected Version(s): * Up to (excluding) 5.6.9 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 28-Nov-2022 | 8.8 | The OWM Weather WordPress plugin before 5.6.9 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as contributor<br>**CVE ID : CVE-2022-3769** | N/A | A-UJS-OWM_-121222/587 |
| **Vendor: Veritas** | | | | | |
| **Product: netbackup** | | | | | |
| Affected Version(s): * Up to (including) 10.1 | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 17-Nov-2022 | 8.8 | The Java Admin Console in Veritas NetBackup through 10.1 and related Veritas products on Linux and UNIX allows authenticated non-root users (that have been explicitly added to the auth.conf file) to | https://www.veritas.com/content/support/en_US/security/VTS22-015 | A-VER-NETB-121222/588 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | execute arbitrary commands as root.<br>**CVE ID : CVE-2022-45461** | | |
| **Vendor: video_thumbnails_project** | | | | | |
| **Product: video_thumbnails** | | | | | |
| Affected Version(s): * Up to (including) 2.12.3 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The Video Thumbnails WordPress plugin through 2.12.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3828** | N/A | A-VID-VIDE-121222/589 |
| **Vendor: villatheme** | | | | | |
| **Product: s2w_-_import_shopify_to_woocommerce** | | | | | |
| Affected Version(s): * Up to (including) 1.1.12 | | | | | |
| N/A | 18-Nov-2022 | 4.9 | Auth. (admin+) Arbitrary File Read vulnerability in S2W – Import Shopify to WooCommerce plugin <= 1.1.12 on WordPress.<br>**CVE ID : CVE-2022-44634** | https://wordpress.org/plugins/import-shopify-to-woocommerce/#developers | A-VIL-S2W_-121222/590 |
| **Vendor: visztpeter** | | | | | |
| **Product: integration_for_szamlazz.hu_\&_woocommerce** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (excluding) 5.6.3.3 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Viszt Péter's Integration for Szamlazz.hu & WooCommerce plugin <= 5.6.3.2 and Csomagpontok és szállítási címkék WooCommerce-hez plugin <= 1.9.0.2 on WordPress.<br>**CVE ID : CVE-2022-41685** | https://patchstack.com/database/vulnerability/integration-for-szamlazzhu-woocommerce/wordpress-integration-for-szamlazz-hu-woocommerce-plugin-5-6-3-2-multiple-cross-site-request-forgery-csrf-vulnerabilities?_s_id=cve | A-VIS-INTE-121222/591 |
| **Product: package_points_and_shipping_labels_for_woocommerce** | | | | | |
| Affected Version(s): * Up to (excluding) 1.9.0.3 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 8.8 | Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Viszt Péter's Integration for Szamlazz.hu & WooCommerce plugin <= 5.6.3.2 and Csomagpontok és szállítási címkék WooCommerce-hez plugin <= 1.9.0.2 on WordPress.<br>**CVE ID : CVE-2022-41685** | https://patchstack.com/database/vulnerability/integration-for-szamlazzhu-woocommerce/wordpress-integration-for-szamlazz-hu-woocommerce-plugin-5-6-3-2-multiple-cross-site-request-forgery-csrf-vulnerabilities?_s_id=cve | A-VIS-PACK-121222/592 |
| **Vendor: watchtowerhq** | | | | | |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: watchtower** | | | | | |
| Affected Version(s): * Up to (including) 3.6.15 | | | | | |
| Missing Authorization | 18-Nov-2022 | 9.1 | Unauth. Arbitrary File Deletion vulnerability in WatchTowerHQ plugin <= 3.6.15 on WordPress.<br>**CVE ID : CVE-2022-44584** | https://patchstack.com/database/vulnerability/watchtowerhq/wordpress-watchtowerhq-plugin-3-6-15-unauth-arbitrary-file-deletion-vulnerability?_s_id=cve, https://wordpress.org/plugins/watchtowerhq/#developers | A-WAT-WATC-121222/593 |
| Files or Directories Accessible to External Parties | 18-Nov-2022 | 7.5 | Unauth. Arbitrary File Download vulnerability in WatchTowerHQ plugin <= 3.6.15 on WordPress.<br>**CVE ID : CVE-2022-44583** | https://wordpress.org/plugins/watchtowerhq/#developers, https://patchstack.com/database/vulnerability/watchtowerhq/wordpress-watchtowerhq-plugin-3-6-15-unauth-arbitrary-file-download-vulnerability?_s_id=cve | A-WAT-WATC-121222/594 |
| **Vendor: Wbce** | | | | | |
| **Product: wbce_cms** | | | | | |
| Affected Version(s): * Up to (including) 1.5.4 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in the Modify Page module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Source field.<br>**CVE ID : CVE-2022-45012** | N/A | A-WBC-WBCE-121222/595 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in the Show Advanced Option module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Section Header field.<br>**CVE ID : CVE-2022-45013** | N/A | A-WBC-WBCE-121222/596 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Results Header field.<br>**CVE ID : CVE-2022-45014** | N/A | A-WBC-WBCE-121222/597 |
| Improper Neutralization of Input During | 21-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers | N/A | A-WBC-WBCE-121222/598 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | to execute arbitrary web scripts or HTML via a crafted payload injected into the Results Footer field.<br>**CVE ID : CVE-2022-45015** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Footer field.<br>**CVE ID : CVE-2022-45016** | N/A | A-WBC-WBCE-121222/599 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Nov-2022 | 4.8 | A cross-site scripting (XSS) vulnerability in the Overview Page settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Post Loop field.<br>**CVE ID : CVE-2022-45017** | N/A | A-WBC-WBCE-121222/600 |
| Affected Version(s): 1.5.4 | | | | | |
| Unrestricted Upload of File with Dangerous Type | 25-Nov-2022 | 7.2 | An arbitrary file upload vulnerability in the Server Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary code via a crafted PHP file. | N/A | A-WBC-WBCE-121222/601 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-45039** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 5.4 | A cross-site scripting (XSS) vulnerability in the Search Settings module of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the No Results field.<br>**CVE ID : CVE-2022-45036** | N/A | A-WBC-WBCE-121222/602 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 5.4 | A cross-site scripting (XSS) vulnerability in /admin/users/index.php of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Display Name field.<br>**CVE ID : CVE-2022-45037** | N/A | A-WBC-WBCE-121222/603 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Nov-2022 | 5.4 | A cross-site scripting (XSS) vulnerability in /admin/settings/save.php of WBCE CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Website Footer field.<br>**CVE ID : CVE-2022-45038** | N/A | A-WBC-WBCE-121222/604 |
| Improper Neutralization of Input | 25-Nov-2022 | 5.4 | A cross-site scripting (XSS) vulnerability in /admin/pages/sections_save.php of WBCE | N/A | A-WBC-WBCE-121222/605 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | CMS v1.5.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name Section field.<br>**CVE ID : CVE-2022-45040** | | |
| **Vendor: web-based_student_clearance_system_project** | | | | | |
| **Product: web-based_student_clearance_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | Web-Based Student Clearance System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in changepassword.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtnew_password parameter.<br>**CVE ID : CVE-2022-45221** | N/A | A-WEB-WEB--121222/606 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | Web-Based Student Clearance System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /Admin/add-student.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into | N/A | A-WEB-WEB--121222/607 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the txtfullname parameter.<br>**CVE ID : CVE-2022-45223** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | Web-Based Student Clearance System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in Admin/add-admin.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtfullname parameter.<br>**CVE ID : CVE-2022-45224** | N/A | A-WEB-WEB--121222/608 |
| **Vendor: webartesanal** | | | | | |
| **Product: mantenimiento_web** | | | | | |
| Affected Version(s): * Up to (excluding) 0.14 | | | | | |
| Cross-Site Request Forgery (CSRF) | 18-Nov-2022 | 6.1 | Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS) in Mantenimiento web plugin <= 0.13 on WordPress.<br>**CVE ID : CVE-2022-38075** | https://patchstack.com/database/vulnerability/mantenimiento-web/wordpress-mantenimiento-web-plugin-0-13-cross-site-request-forgery-csrf-vulnerability-leading-to-stored-cross-site-scripting-xss?_s_id=cve | A-WEB-MANT-121222/609 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: webence** | | | | | |
| **Product: iq_block_country** | | | | | |
| Affected Version(s): * Up to (excluding) 1.2.19 | | | | | |
| Incorrect Authorization | 19-Nov-2022 | 9.8 | Block BYPASS vulnerability in iQ Block Country plugin <= 1.2.18 on WordPress.<br>**CVE ID : CVE-2022-41155** | https://wordpress.org/plugins/iq-block-country/#developers, https://patchstack.com/database/vulnerability/iq-block-country/wordpress-iq-block-country-plugin-1-2-18-block-bypass-vulnerability?_s_id=cve | A-WEB-IQ_B-121222/610 |
| **Vendor: webpsilon** | | | | | |
| **Product: ultimate_tables** | | | | | |
| Affected Version(s): * Up to (including) 1.6.5 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Nov-2022 | 6.1 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ULTIMATE TABLES plugin <= 1.6.5 on WordPress.<br>**CVE ID : CVE-2022-36357** | https://patchstack.com/database/vulnerability/ultimate-tables/wordpress-ultimate-tables-plugin-1-6-5-unauth-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve | A-WEB-ULTI-121222/611 |
| **Vendor: webvendome_project** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: webvendome** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Nov-2022 | 9.8 | Webvendome - Webvendome SQL Injection. SQL Injection in the Parameter " DocNumber" Request : Get Request : /webvendome/showfiles.aspx?jobnumber=nullDoc Number=HERE.<br>**CVE ID : CVE-2022-36787** | N/A | A-WEB-WEBV-121222/612 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Nov-2022 | 5.3 | Webvendome - Webvendome Internal Server IP Disclosure. Send GET Request to the request which is shown in the picture. Internal Server IP and Full path disclosure.<br>**CVE ID : CVE-2022-39178** | N/A | A-WEB-WEBV-121222/613 |
| **Vendor: web_based_quiz_system_project** | | | | | |
| **Product: web_based_quiz_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Cleartext Transmission of Sensitive Information | 25-Nov-2022 | 7.5 | Web Based Quiz System v1.0 transmits user passwords in plaintext during the authentication process, allowing attackers to obtain users' passwords via a bruteforce attack.<br>**CVE ID : CVE-2022-44411** | N/A | A-WEB-WEB_-121222/614 |
| **Vendor: wire** | | | | | |
| **Product: wire** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (including) 3.22.3993 | | | | | |
| Insertion of Sensitive Information into Log File | 18-Nov-2022 | 4.7 | Wire through 3.22.3993 on Windows advertises deletion of sent messages; nonetheless, all messages can be retrieved (for a limited period of time) from the AppData\Roaming\Wire\IndexedDB\https_app.wire.com_0.indexeddb.leveldb database.<br>**CVE ID : CVE-2022-43673** | N/A | A-WIR-WIRE-121222/615 |
| **Vendor: withsecure** | | | | | |
| **Product: f-secure_policy_manager** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 17-Nov-2022 | 9.8 | Arbitrary file write in F-Secure Policy Manager through 2022-08-10 allows unauthenticated users to write the file with the contents in arbitrary locations on the F-Secure Policy Manager Server.<br>**CVE ID : CVE-2022-38165** | https://www.withsecure.com/en/support/security-advisories/cve-2022-38165 | A-WIT-F-SE-121222/616 |
| **Vendor: Wondercms** | | | | | |
| **Product: wondercms** | | | | | |
| Affected Version(s): 3.3.4 | | | | | |
| Improper Neutralization of Input During | 17-Nov-2022 | 6.1 | A cross-site scripting (XSS) vulnerability in Wondercms v3.3.4 allows attackers to execute arbitrary web | N/A | A-WON-WOND-121222/617 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | scripts or HTML via a crafted payload injected into the Site title field of the Configuration Panel.<br>**CVE ID : CVE-2022-43332** | | |
| **Vendor: wordplus** | | | | | |
| **Product: better_messages** | | | | | |
| Affected Version(s): * Up to (excluding) 1.9.10.69 | | | | | |
| Server-Side Request Forgery (SSRF) | 19-Nov-2022 | 8.8 | Auth. (subscriber+) Server-Side Request Forgery (SSRF) vulnerability in Better Messages plugin 1.9.10.68 on WordPress.<br>**CVE ID : CVE-2022-41609** | https://patchstack.com/database/vulnerability/bp-better-messages/wordpress-better-messages-plugin-1-9-10-68-server-side-request-forgery-ssrf-vulnerability?_s_id=cve, https://wordpress.org/plugins/bp-better-messages/#developers | A-WOR-BETT-121222/618 |
| Affected Version(s): * Up to (excluding) 1.9.10.71 | | | | | |
| Incorrect Authorization | 18-Nov-2022 | 6.5 | Auth. (subscriber+) Messaging Block Bypass vulnerability in Better Messages plugin <= 1.9.10.69 on WordPress.<br>**CVE ID : CVE-2022-40216** | https://wordpress.org/plugins/bp-better-messages/#developers, https://patchstack.com/database/vulnerability/bp- | A-WOR-BETT-121222/619 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | better-messages/wordpress-better-messages-plugin-1-9-10-69-messaging-block-bypass-vulnerability?_s_id=cve | |
| **Vendor: wp-polls_project** | | | | | |
| **Product: wp-polls** | | | | | |
| Affected Version(s): * Up to (excluding) 2.76.0 | | | | | |
| Authorization Bypass Through User-Controlled Key | 21-Nov-2022 | 5.3 | The WP-Polls WordPress plugin before 2.76.0 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based limitations to vote in certain situations.<br>**CVE ID : CVE-2022-1581** | https://wpscan.com/vulnerability/c1896ab9-9585-40e2-abbf-ef5153b3c6b2 | A-WP--WP-P-121222/620 |
| Affected Version(s): * Up to (excluding) 2.77.0 | | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 18-Nov-2022 | 3.1 | Auth. (subscriber+) Race Condition vulnerability in WP-Polls plugin <= 2.76.0 on WordPress.<br>**CVE ID : CVE-2022-40130** | https://patchstack.com/database/vulnerability/wp-polls/wordpress-wp-polls-plugin-2-76-0-race-condition-vulnerability?_s_id=cve, https://word | A-WP--WP-P-121222/621 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | press.org/plugins/wp-polls/#developers | |
| **Vendor: wpbrigade** | | | | | |
| **Product: loginpress** | | | | | |
| Affected Version(s): * Up to (including) 1.6.2 | | | | | |
| N/A | 18-Nov-2022 | 5.3 | Broken Access Control vulnerability in WordPress LoginPress plugin <= 1.6.2 on WordPress leading to unauth. changing of Opt-In or Opt-Out tracking settings.<br>**CVE ID : CVE-2022-41839** | https://patchstack.com/database/vulnerability/loginpress/wordpress-loginpress-plugin-1-6-2-broken-access-control-vulnerability?_s_id=cve | A-WPB-LOGI-121222/622 |
| **Vendor: wpchill** | | | | | |
| **Product: customizable_wordpress_gallery_plugin_-_modula_image_gallery** | | | | | |
| Affected Version(s): * Up to (excluding) 2.6.91 | | | | | |
| N/A | 18-Nov-2022 | 5.3 | Unauth. Plugin Settings Change vulnerability in Modula plugin <= 2.6.9 on WordPress.<br>**CVE ID : CVE-2022-41135** | https://patchstack.com/database/vulnerability/modula-best-grid-gallery/wordpress-modula-plugin-2-6-9-unauth-plugin-settings-change-vulnerability?_s_id=cve | A-WPC-CUST-121222/623 |
| **Vendor: Wpml** | | | | | |
| **Product: wpml** | | | | | |
| Affected Version(s): * Up to (excluding) 4.5.14 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF) | 17-Nov-2022 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in WPML Multilingual CMS premium plugin <= 4.5.13 on WordPress.<br>**CVE ID : CVE-2022-45071** | https://patchstack.com/database/vulnerability/sitepress-multilingual-cms/wordpress-wpml-multilingual-cms-premium-plugin-4-5-13-cross-site-request-forgery-csrf-vulnerability?_s_id=cve | A-WPM-WPML-121222/624 |
| Cross-Site Request Forgery (CSRF) | 17-Nov-2022 | 4.3 | Cross-Site Request Forgery (CSRF) vulnerability in WPML Multilingual CMS premium plugin <= 4.5.13 on WordPress.<br>**CVE ID : CVE-2022-45072** | https://patchstack.com/database/vulnerability/sitepress-multilingual-cms/wordpress-wpml-multilingual-cms-premium-plugin-4-5-13-cross-site-request-forgery-csrf-vulnerability-2?_s_id=cve | A-WPM-WPML-121222/625 |
| Affected Version(s): * Up to (including) 4.5.10 | | | | | |
| Incorrect Permission Assignment for Critical Resource | 17-Nov-2022 | 4.3 | Broken Access Control vulnerability in WPML Multilingual CMS premium plugin <= 4.5.10 on WordPress allows users with a subscriber or higher user role to change | https://patchstack.com/database/vulnerability/sitepress-multilingual-cms/wordpress-wpml- | A-WPM-WPML-121222/626 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | plugin settings (selected language for legacy widgets, the default behavior for media content).<br>**CVE ID : CVE-2022-38461** | multilingual-cms-plugin-4-5-10-broken-access-control-vulnerability?_s_id=cve | |
| N/A | 18-Nov-2022 | 4.3 | Broken Access Control vulnerability in WPML Multilingual CMS premium plugin <= 4.5.10 on WordPress allows users with subscriber or higher user roles to change the status of the translation jobs.<br>**CVE ID : CVE-2022-38974** | https://patchstack.com/database/vulnerability/sitepress-multilingual-cms/wordpress-wpml-multilingual-cms-plugin-4-5-10-broken-access-control-vulnerability-2?_s_id=cve | A-WPM-WPML-121222/627 |
| **Vendor: wpsmartcontracts** | | | | | |
| **Product: wpsmartcontracts** | | | | | |
| Affected Version(s): * Up to (excluding) 1.3.12 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 28-Nov-2022 | 8.8 | The WPSmartContracts WordPress plugin before 1.3.12 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as author<br>**CVE ID : CVE-2022-3768** | N/A | A-WPS-WPSM-121222/628 |
| **Vendor: wp_admin_ui_customize_project** | | | | | |
| **Product: wp_admin_ui_customize** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (excluding) 1.5.13 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 28-Nov-2022 | 4.8 | The WP Admin UI Customize WordPress plugin before 1.5.13 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).<br>**CVE ID : CVE-2022-3824** | N/A | A-WP_-WP_A-121222/629 |
| **Vendor: wp_user_merger_project** | | | | | |
| **Product: wp_user_merger** | | | | | |
| Affected Version(s): * Up to (excluding) 1.5.3 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 28-Nov-2022 | 8.8 | The WP User Merger WordPress plugin before 1.5.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as admin<br>**CVE ID : CVE-2022-3848** | N/A | A-WP_-WP_U-121222/630 |
| Improper Neutralization of Special Elements used in an | 28-Nov-2022 | 8.8 | The WP User Merger WordPress plugin before 1.5.3 does not properly sanitise and escape a parameter before using it in a | N/A | A-WP_-WP_U-121222/631 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| SQL Command ('SQL Injection') | | | SQL statement, leading to a SQL injection exploitable by users with a role as low as admin<br>**CVE ID : CVE-2022-3849** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 28-Nov-2022 | 8.8 | The WP User Merger WordPress plugin before 1.5.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as admin<br>**CVE ID : CVE-2022-3865** | N/A | A-WP_-WP_U-121222/632 |
| **Vendor: Xmlsoft** | | | | | |
| **Product: libxml2** | | | | | |
| Affected Version(s): * Up to (excluding) 2.10.3 | | | | | |
| Integer Overflow or Wraparound | 23-Nov-2022 | 7.5 | An issue was discovered in libxml2 before 2.10.3. When parsing a multi-gigabyte XML document with the XML_PARSE_HUGE parser option enabled, several integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leading to a segmentation fault.<br>**CVE ID : CVE-2022-40303** | https://gitlab.gnome.org/GNOME/libxml2/-/commit/c846986356fc149915a74972bf198abc266bc2c0 | A-XML-LIBX-121222/633 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: xuxueli** | | | | | |
| **Product: xxl-job** | | | | | |
| Affected Version(s): * Up to (including) 2.3.1 | | | | | |
| Server-Side Request Forgery (SSRF) | 17-Nov-2022 | 8.8 | XXL-Job before v2.3.1 contains a Server-Side Request Forgery (SSRF) via the component /admin/controller/JobLogController.java.<br>**CVE ID : CVE-2022-43183** | N/A | A-XUX-XXL--121222/634 |
| **Vendor: Xwiki** | | | | | |
| **Product: Xwiki** | | | | | |
| Affected Version(s): * Up to (excluding) 13.10.8 | | | | | |
| Missing Authorization | 22-Nov-2022 | 8.1 | XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The application allows anyone with view access to modify any page of the wiki by importing a crafted XAR package. The problem has been patched in XWiki 14.6RC1, 14.6 and 13.10.8. As a workaround, setting the right of the page Filter.WebHome and making sure only the main wiki administrators can view the application installed on main wiki or edit the page and apply the changed | https://jira.xwiki.org/browse/XWIKI-19758, https://github.com/xwiki/xwiki-platform/commit/fb49b4f289ee28e45cfada8e97e320cd3ed27113, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-q6jp-gcww-8v2j | A-XWI-XWIK-121222/635 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | described in commit fb49b4f.<br>**CVE ID : CVE-2022-41937** | | |
| Affected Version(s): 14.5 | | | | | |
| Missing Authorization | 22-Nov-2022 | 8.1 | XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The application allows anyone with view access to modify any page of the wiki by importing a crafted XAR package. The problem has been patched in XWiki 14.6RC1, 14.6 and 13.10.8. As a workaround, setting the right of the page Filter.WebHome and making sure only the main wiki administrators can view the application installed on main wiki or edit the page and apply the changed described in commit fb49b4f.<br>**CVE ID : CVE-2022-41937** | https://jira.xwiki.org/browse/XWIKI-19758, https://github.com/xwiki/xwiki-platform/commit/fb49b4f289ee28e45cfada8e97e320cd3ed27113, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-q6jp-gcww-8v2j | A-XWI-XWIK-121222/636 |
| Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.3 | | | | | |
| Missing Authorization | 22-Nov-2022 | 8.1 | XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The | https://jira.xwiki.org/browse/XWIKI-19758, https://github.com/xwiki/ | A-XWI-XWIK-121222/637 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | application allows anyone with view access to modify any page of the wiki by importing a crafted XAR package. The problem has been patched in XWiki 14.6RC1, 14.6 and 13.10.8. As a workaround, setting the right of the page Filter.WebHome and making sure only the main wiki administrators can view the application installed on main wiki or edit the page and apply the changed described in commit fb49b4f.<br>**CVE ID : CVE-2022-41937** | xwiki-platform/commit/fb49b4f289ee28e45cfada8e97e320cd3ed27113, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-q6jp-gcww-8v2j | |
| Exposure of Private Personal Information to an Unauthorized Actor | 22-Nov-2022 | 7.5 | XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The `modifications` rest endpoint does not filter out entries according to the user's rights. Therefore, information hidden from unauthorized users are exposed though the `modifications` rest endpoint (comments and page names etc). Users should upgrade | https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-p88w-fhxw-xvcc, https://jira.xwiki.org/browse/XWIKI-19997, https://github.com/xwiki/xwiki-platform/commit/38dc1aa1a4435f24d58f | A-XWI-XWIK-121222/638 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to XWiki 14.6+, 14.4.3+, or 13.10.8+. Older versions have not been patched. There are no known workarounds.<br>**CVE ID : CVE-2022-41936** | 5b8e4566cbcb0971f8ff | |
| Affected Version(s): From (including) 14.5 Up to (excluding) 14.6 | | | | | |
| Exposure of Private Personal Information to an Unauthorized Actor | 22-Nov-2022 | 7.5 | XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The `modifications` rest endpoint does not filter out entries according to the user's rights. Therefore, information hidden from unauthorized users are exposed though the `modifications` rest endpoint (comments and page names etc). Users should upgrade to XWiki 14.6+, 14.4.3+, or 13.10.8+. Older versions have not been patched. There are no known workarounds.<br>**CVE ID : CVE-2022-41936** | https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-p88w-fhxw-xvcc, https://jira.xwiki.org/browse/XWIKI-19997, https://github.com/xwiki/xwiki-platform/commit/38dc1aa1a4435f24d58f5b8e4566cbcb0971f8ff | A-XWI-XWIK-121222/639 |
| Affected Version(s): From (including) 8.1 Up to (excluding) 13.10.8 | | | | | |
| Exposure of Private Personal Information to an | 22-Nov-2022 | 7.5 | XWiki Platform is a generic wiki platform offering runtime services for applications built on | https://github.com/xwiki/xwiki-platform/security/advisorie | A-XWI-XWIK-121222/640 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unauthorized Actor | | | top of it. The `modifications` rest endpoint does not filter out entries according to the user's rights. Therefore, information hidden from unauthorized users are exposed though the `modifications` rest endpoint (comments and page names etc). Users should upgrade to XWiki 14.6+, 14.4.3+, or 13.10.8+. Older versions have not been patched. There are no known workarounds.<br>**CVE ID : CVE-2022-41936** | s/GHSA-p88w-fhxw-xvcc, https://jira.xwiki.org/browse/XWIKI-19997, https://github.com/xwiki/xwiki-platform/commit/38dc1aa1a4435f24d58f5b8e4566cbcb0971f8ff | |
| **Vendor: yikesinc** | | | | | |
| **Product: custom_product_tabs_for_woocommerce** | | | | | |
| Affected Version(s): * Up to (excluding) 1.8.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Nov-2022 | 4.8 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Custom Product Tabs for WooCommerce plugin <= 1.7.9 on WordPress.<br>**CVE ID : CVE-2022-43463** | https://patchstack.com/database/vulnerability/yikes-inc-easy-custom-woocommerce-product-tabs/wordpress-custom-product-tabs-for-woocommerce-plugin-1-7-9-auth-stored-cross-site-scripting- | A-YIK-CUST-121222/641 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | xss-vulnerability?_s_id=cve | |
| **Vendor: Zohocorp** | | | | | |
| **Product: manageengine_admanager_plus** | | | | | |
| Affected Version(s): * Up to (excluding) 7.1 | | | | | |
| N/A | 18-Nov-2022 | 7.2 | Zoho ManageEngine ADManager Plus through 7151 allows authenticated admin users to execute the commands in proxy settings.<br>**CVE ID : CVE-2022-42904** | https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2022-42904.html | A-ZOH-MANA-121222/642 |
| Affected Version(s): 7.1 | | | | | |
| N/A | 18-Nov-2022 | 7.2 | Zoho ManageEngine ADManager Plus through 7151 allows authenticated admin users to execute the commands in proxy settings.<br>**CVE ID : CVE-2022-42904** | https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2022-42904.html | A-ZOH-MANA-121222/643 |
| **Product: manageengine_assetexplorer** | | | | | |
| Affected Version(s): * Up to (excluding) 6.9 | | | | | |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.<br>**CVE ID : CVE-2022-40772** | https://manageengine.com,<br>https://www.manageengine.com/products/service-desk/CVE-2022-40772.html | A-ZOH-MANA-121222/644 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/645 |
| Affected Version(s): 6.9 | | | | | |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.<br>**CVE ID : CVE-2022-40772** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40772.html | A-ZOH-MANA-121222/646 |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/647 |
| **Product: manageengine_servicedesk_plus** | | | | | |
| Affected Version(s): 14.0 | | | | | |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module. | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE- | A-ZOH-MANA-121222/648 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-40772** | 2022-40772.html | |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/649 |
| Affected Version(s): * Up to (excluding) 13.0 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 7.2 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated command injection. This can be exploited by high-privileged users.<br>**CVE ID : CVE-2022-40770** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40770.html | A-ZOH-MANA-121222/650 |
| Affected Version(s): * Up to (excluding) 14.0 | | | | | |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.<br>**CVE ID : CVE-2022-40772** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40772.html | A-ZOH-MANA-121222/651 |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that | https://manageengine.com, https://www.manageengine.com/products/service- | A-ZOH-MANA-121222/652 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | desk/CVE-2022-40771.html | |
| Affected Version(s): 13.0 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 7.2 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated command injection. This can be exploited by high-privileged users.<br>**CVE ID : CVE-2022-40770** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40770.html | A-ZOH-MANA-121222/653 |
| **Product: manageengine_servicedesk_plus_msp** | | | | | |
| Affected Version(s): * Up to (excluding) 13.0 | | | | | |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/654 |
| Affected Version(s): 13.0 | | | | | |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/655 |
| Affected Version(s): * Up to (excluding) 10.6 | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 7.2 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated command injection. This can be exploited by high-privileged users.<br>**CVE ID : CVE-2022-40770** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40770.html | A-ZOH-MANA-121222/656 |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.<br>**CVE ID : CVE-2022-40772** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40772.html | A-ZOH-MANA-121222/657 |
| Affected Version(s): 10.6 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 7.2 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated command injection. This can be exploited by high-privileged users.<br>**CVE ID : CVE-2022-40770** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40770.html | A-ZOH-MANA-121222/658 |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module. | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE- | A-ZOH-MANA-121222/659 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-40772** | 2022-40772.html | |
| **Product: manageengine_supportcenter_plus** | | | | | |
| Affected Version(s): * Up to (excluding) 11.0 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 7.2 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated command injection. This can be exploited by high-privileged users.<br>**CVE ID : CVE-2022-40770** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40770.html | A-ZOH-MANA-121222/660 |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.<br>**CVE ID : CVE-2022-40772** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40772.html | A-ZOH-MANA-121222/661 |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com, https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/662 |
| Affected Version(s): 11.0 | | | | | |
| Improper Neutralization of Special Elements | 23-Nov-2022 | 7.2 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to authenticated | https://manageengine.com, https://www.manageengine.com/produc | A-ZOH-MANA-121222/663 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in a Command ('Command Injection') | | | command injection. This can be exploited by high-privileged users.<br>**CVE ID : CVE-2022-40770** | ts/service-desk/CVE-2022-40770.html | |
| Improper Privilege Management | 23-Nov-2022 | 6.5 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to a validation bypass that allows users to access sensitive data via the report module.<br>**CVE ID : CVE-2022-40772** | https://manageengine.com,<br>https://www.manageengine.com/products/service-desk/CVE-2022-40772.html | A-ZOH-MANA-121222/664 |
| Improper Restriction of XML External Entity Reference | 23-Nov-2022 | 4.9 | Zoho ManageEngine ServiceDesk Plus versions 13010 and prior are vulnerable to an XML External Entity attack that leads to Information Disclosure.<br>**CVE ID : CVE-2022-40771** | https://manageengine.com,<br>https://www.manageengine.com/products/service-desk/CVE-2022-40771.html | A-ZOH-MANA-121222/665 |
| Incorrect Authorization | 17-Nov-2022 | 3.3 | Zoho ManageEngine SupportCenter Plus through 11024 allows low-privileged users to view the organization users list.<br>**CVE ID : CVE-2022-42903** | https://www.manageengine.com/products/support-center/cve-2022-42903.html | A-ZOH-MANA-121222/666 |
| **Vendor: Zoom** | | | | | |
| **Product: meetings** | | | | | |
| Affected Version(s): * Up to (excluding) 5.12.6 | | | | | |
| Concurrent Execution using | 17-Nov-2022 | 7.8 | The Zoom Client for Meetings Installer for macOS (Standard and | https://explore.zoom.us/en/trust/securit | A-ZOO-MEET-121222/667 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | for IT Admin) before version 5.12.6 contains a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability during the install process to escalate their privileges to root.<br>**CVE ID : CVE-2022-28768** | y/security-bulletin/ | |
| Uncontrolled Search Path Element | 17-Nov-2022 | 7.3 | Windows 32-bit versions of the Zoom Client for Meetings before 5.12.6 and Zoom Rooms for Conference Room before version 5.12.6 are susceptible to a DLL injection vulnerability. A local low-privileged user could exploit this vulnerability to run arbitrary code in the context of the Zoom client.<br>**CVE ID : CVE-2022-28766** | https://explore.zoom.us/en/trust/security/security-bulletin/ | A-ZOO-MEET-121222/668 |
| **Product: rooms** | | | | | |
| Affected Version(s): * Up to (excluding) 5.12.6 | | | | | |
| Uncontrolled Search Path Element | 17-Nov-2022 | 7.8 | The Zoom Rooms Installer for Windows prior to 5.12.6 contains a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability during | https://explore.zoom.us/en/trust/security/security-bulletin/ | A-ZOO-ROOM-121222/669 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the install process to escalate their privileges to the SYSTEM user.<br>**CVE ID : CVE-2022-36924** | | |
| Uncontrolled Search Path Element | 17-Nov-2022 | 7.3 | Windows 32-bit versions of the Zoom Client for Meetings before 5.12.6 and Zoom Rooms for Conference Room before version 5.12.6 are susceptible to a DLL injection vulnerability. A local low-privileged user could exploit this vulnerability to run arbitrary code in the context of the Zoom client.<br>**CVE ID : CVE-2022-28766** | https://explore.zoom.us/en/trust/security/security-bulletin/ | A-ZOO-ROOM-121222/670 |
| **Vendor: Zulip** | | | | | |
| **Product: zulip_server** | | | | | |
| Affected Version(s): From (including) 5.0 Up to (excluding) 5.7 | | | | | |
| Observable Discrepancy | 16-Nov-2022 | 3.7 | Zulip is an open-source team collaboration tool. For organizations with System for Cross-domain Identity Management(SCIM) account management enabled, Zulip Server 5.0 through 5.6 checked the SCIM bearer token using a comparator that did not run in constant time. Therefore, it | https://github.com/zulip/zulip/security/advisories/GHSA-q5gx-377v-w76f,<br>https://github.com/zulip/zulip/commit/59edbfa4113d140d3e20126bc65f4d67b2a8ffe5 | A-ZUL-ZULI-121222/671 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | might theoretically be possible for an attacker to infer the value of the token by performing a sophisticated timing analysis on a large number of failing requests. If successful, this would allow the attacker to impersonate the SCIM client for its abilities to read and update user accounts in the Zulip organization. Organizations where SCIM account management has not been enabled are not affected.<br>**CVE ID : CVE-2022-41914** | | |
| **Hardware** | | | | | |
| **Vendor: ABB** | | | | | |
| **Product: microscada_pro_sys600** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 21-Nov-2022 | 7.8 | An input validation vulnerability exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X SYS600. An authenticated user can launch an administrator level remote code execution irrespective of the authenticated user's role. | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000123&LanguageCode=en&DocumentPartId=&Action=Launch&elqaid=4293&elqat=1 | H-ABB-MICR-121222/672 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | 🟧 | **CVE ID : CVE-2022-3388** | | |
| **Vendor: Carel** | | | | | |
| **Product: boss_mini** | | | | | |
| Affected Version(s): - | | | | | |
| Incorrect Authorization | 18-Nov-2022 | 9.9 | Carel Boss Mini 1.5.0 has Improper Access Control.<br>**CVE ID : CVE-2022-34827** | N/A | H-CAR-BOSS-121222/673 |
| **Vendor: contec** | | | | | |
| **Product: solarview_compact** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | SolarView Compact 6.00 was discovered to contain a command injection vulnerability via network_test.php<br>**CVE ID : CVE-2022-40881** | N/A | H-CON-SOLA-121222/674 |
| **Vendor: Dlink** | | | | | |
| **Product: dir-3060** | | | | | |
| Affected Version(s): a1 | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 18-Nov-2022 | 9.8 | D-Link DIR3060 DIR3060A1_FW111B04.bin is vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44204** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/675 |
| **Product: dir-823g** | | | | | |
| Affected Version(s): - | | | | | |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 9.8 | D-Link DIR823G 1.02B05 is vulnerable to Commad Injection.<br>**CVE ID : CVE-2022-44201** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/676 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 9.8 | A command injection vulnerability has been found on D-Link DIR-823G devices with firmware version 1.02B03 that allows an attacker to execute arbitrary operating system commands through well-designed /HNAP1 requests. Before the HNAP API function can process the request, the system function executes an untrusted command that triggers the vulnerability.<br>**CVE ID : CVE-2022-44808** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/677 |
| **Product: dir-878** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR878 1.02B04 and 1.02B05 are vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44202** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/678 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Authentication | 22-Nov-2022 | 9.8 | D-Link DIR-878 1.02B05 is vulnerable to Incorrect Access Control.<br>**CVE ID : CVE-2022-44801** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/679 |
| **Product: dir-882** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and1.20B06 is vulnerable to Buffer Overflow via the websRedirect function.<br>**CVE ID : CVE-2022-44804** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/680 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44806** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/681 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow via webGetVarString.<br>**CVE ID : CVE-2022-44807** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--121222/682 |
| **Product: dsl-224** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Comman | 17-Nov-2022 | 9.9 | DLINK - DSL-224 Post-auth PCE. DLINK router has an interface where you can configure NTP servers (Network Time Protocol) via jsonrpc API. It is possible to inject a command | N/A | H-DLI-DSL--121222/683 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| d Injection') | | | through this interface that will run with ROOT permissions on the router.<br>**CVE ID : CVE-2022-36786** | | |
| **Product: g_integrated_access_device4** | | | | | |
| Affected Version(s): - | | | | | |
| Incorrect Authorization | 17-Nov-2022 | 7.5 | D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass. *Information Disclosure – file contains a URL with private IP at line 15 "login.asp" A. The window.location.href = http://192.168.1.1/setupWizard.asp" http://192.168.1.1/setupWizard.asp" ; "admin" – contains default username value "login.asp" B. While accessing the web interface, the login form at *Authorization Bypass – URL by "setupWizard.asp' while it blocks direct access to – the web interface does not properly validate user identity variables values located at the client side, it is available to access it without a "login_glag" and "login_status" | N/A | H-DLI-G_IN-121222/684 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | checking browser and to read the admin user credentials for the web interface.<br>**CVE ID : CVE-2022-36785** | | |
| **Vendor: elsight** | | | | | |
| **Product: halo** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 17-Nov-2022 | 9.8 | Elsight – Elsight Halo Remote Code Execution (RCE) Elsight Halo web panel allows us to perform connection validation. through the POST request : /api/v1/nics/wifi/wlan0/ping we can abuse DESTINATION parameter and leverage it to remote code execution.<br>**CVE ID : CVE-2022-36784** | N/A | H-ELS-HALO-121222/685 |
| **Vendor: intelbras** | | | | | |
| **Product: sg_2404_mr** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Privilege Management | 18-Nov-2022 | 7.8 | INTELBRAS SG 2404 MR 20180928-rel64938 allows authenticated attackers to arbitrarily create Administrator accounts via crafted user cookies.<br>**CVE ID : CVE-2022-43308** | N/A | H-INT-SG_2-121222/686 |
| **Product: sg_2404_poe** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Privilege Management | 18-Nov-2022 | 7.8 | INTELBRAS SG 2404 MR 20180928-rel64938 allows authenticated attackers to arbitrarily create Administrator accounts via crafted user cookies.<br>**CVE ID : CVE-2022-43308** | N/A | H-INT-SG_2-121222/687 |
| **Vendor: m5t** | | | | | |
| **Product: mediatrix_4102s** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 17-Nov-2022 | 6.8 | Mediatrix 4102 before v48.5.2718 allows local attackers to gain root access via the UART port.<br>**CVE ID : CVE-2022-43096** | https://documentation.media5corp.com/display/MP/DGW+Security+Improvement+Notes+v48.5.2718 | H-M5T-MEDI-121222/688 |
| **Vendor: Netgear** | | | | | |
| **Product: r7000p** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter wan_dns1_sec.<br>**CVE ID : CVE-2022-44184** | https://www.netgear.com/about/security/ | H-NET-R700-121222/689 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter wan_dns1_pri. | https://www.netgear.com/about/security/ | H-NET-R700-121222/690 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-44186** | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via wan_dns1_pri.<br>**CVE ID : CVE-2022-44187** | https://www.netgear.com/about/security/ | H-NET-R700-121222/691 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter enable_band_steering.<br>**CVE ID : CVE-2022-44188** | https://www.netgear.com/about/security/ | H-NET-R700-121222/692 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter enable_band_steering.<br>**CVE ID : CVE-2022-44190** | https://www.netgear.com/about/security/ | H-NET-R700-121222/693 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameters KEY1 and KEY2.<br>**CVE ID : CVE-2022-44191** | https://www.netgear.com/about/security/ | H-NET-R700-121222/694 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameters: starthour, startminute , endhour, and endminute.<br>**CVE ID : CVE-2022-44193** | https://www.netgear.com/about/security/ | H-NET-R700-121222/695 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameters apmode_dns1_pri and apmode_dns1_sec.<br>**CVE ID : CVE-2022-44194** | http://netgear.com, https://www.netgear.com/about/security/ | H-NET-R700-121222/696 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameter openvpn_push1.<br>**CVE ID : CVE-2022-44196** | https://www.netgear.com/about/security/ | H-NET-R700-121222/697 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameter openvpn_server_ip.<br>**CVE ID : CVE-2022-44197** | https://www.netgear.com/about/security/ | H-NET-R700-121222/698 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter openvpn_push1.<br>**CVE ID : CVE-2022-44198** | https://www.netgear.com/about/security/ | H-NET-R700-121222/699 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter openvpn_server_ip.<br>**CVE ID : CVE-2022-44199** | https://www.netgear.com/about/security/ | H-NET-R700-121222/700 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8, V1.3.1.64 is vulnerable to Buffer Overflow via parameters: | https://www.netgear.com/about/security/ | H-NET-R700-121222/701 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | stamode_dns1_pri and stamode_dns1_sec.<br>**CVE ID : CVE-2022-44200** | | |
| **Vendor: Nvidia** | | | | | |
| **Product: geforce** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/702 |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/703 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | | |
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/704 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/705 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-31610** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/706 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/707 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a | https://nvidia.custhelp.com/app/answers | H-NVI-GEFO-121222/708 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | /detail/a_id/5383 |  |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/709 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-GEFO-121222/710 |
| NULL Pointer | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux | https://nvidia.custhelp.com | H-NVI-GEFO-121222/711 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Dereference | | | contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | /app/answers/detail/a_id/5383 | |
| **Product: tesla** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/712 |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/713 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | | |
| Improper Preservation of Permissions | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in an optional D-Bus configuration file, where a local user with basic capabilities can impact protected D-Bus endpoints, which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.<br>**CVE ID : CVE-2022-31608** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/714 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/715 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/716 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/717 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-31612** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure.<br>**CVE ID : CVE-2022-31616** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/718 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/719 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/720 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 5.5 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-31615** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | H-NVI-TESL-121222/721 |
| **Vendor: nxp** | | | | | |
| **Product: i.mx_6** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP | N/A | H-NXP-I.MX-121222/722 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6dual** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the | N/A | H-NXP-I.MX-121222/723 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_6duallite** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for | N/A | H-NXP-I.MX-121222/724 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6dualplus** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | H-NXP-I.MX-121222/725 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: i.mx_6quad** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | H-NXP-I.MX-121222/726 |
| **Product: i.mx_6quadplus** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | H-NXP-I.MX-121222/727 |
| **Product: i.mx_6solo** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in | N/A | H-NXP-I.MX-121222/728 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6sololite** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT | N/A | H-NXP-I.MX-121222/729 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6solox** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device | N/A | H-NXP-I.MX-121222/730 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6ull** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically | N/A | H-NXP-I.MX-121222/731 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6ultralite** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended | N/A | H-NXP-I.MX-121222/732 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_6ulz** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable | N/A | H-NXP-I.MX-121222/733 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_7dual** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.) | N/A | H-NXP-I.MX-121222/734 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | **CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_7solo** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | H-NXP-I.MX-121222/735 |
| **Product: i.mx_7ulp** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | H-NXP-I.MX-121222/736 |
| **Product: i.mx_8m_mini** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in | N/A | H-NXP-I.MX-121222/737 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_8m_quad** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT | N/A | H-NXP-I.MX-121222/738 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_8m_vybrid** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device | N/A | H-NXP-I.MX-121222/739 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_rt1010** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically | N/A | H-NXP-I.MX-121222/740 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1015** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended | N/A | H-NXP-I.MX-121222/741 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1020** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable | N/A | H-NXP-I.MX-121222/742 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1050** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.) | N/A | H-NXP-I.MX-121222/743 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1060** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | H-NXP-I.MX-121222/744 |
| **Vendor: Realtek** | | | | | |
| **Product: rtl8111ep-cg** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Use of Hard-coded Credentials | 29-Nov-2022 | 2.1 | RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated physical attacker can use the hard-coded default password during system reboot triggered by other user, to acquire partial system information such as serial number and server information.<br>**CVE ID : CVE-2022-32967** | N/A | H-REA-RTL8-121222/745 |
| **Product: rtl8111fp-cg** | | | | | |
| Affected Version(s): - | | | | | |
| Missing Authorization | 29-Nov-2022 | 6.5 | RTL8168FP-CG Dash remote management function has missing authorization. An unauthenticated attacker within the adjacent network can connect to DASH service port to disrupt service.<br>**CVE ID : CVE-2022-32966** | N/A | H-REA-RTL8-121222/746 |
| Use of Hard-coded Credentials | 29-Nov-2022 | 2.1 | RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated physical attacker can use the hard-coded default password during system reboot triggered by other | N/A | H-REA-RTL8-121222/747 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | user, to acquire partial system information such as serial number and server information.<br>**CVE ID : CVE-2022-32967** | | |
| **Vendor: Tenda** | | | | | |
| **Product: ac15** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetIpMacBind.<br>**CVE ID : CVE-2022-44156** | N/A | H-TEN-AC15-121222/748 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.18 is avulnerable to Buffer Overflow via function formSetPPTPServer.<br>**CVE ID : CVE-2022-44167** | N/A | H-TEN-AC15-121222/749 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.18 is vulnerable to Buffer Overflow via function fromSetRouteStatic..<br>**CVE ID : CVE-2022-44168** | N/A | H-TEN-AC15-121222/750 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.18 is vulnerable to Buffer Overflow via function formSetVirtualSer.<br>**CVE ID : CVE-2022-44169** | N/A | H-TEN-AC15-121222/751 |
| **Product: ac18** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function form_fast_setting_wifi_set.<br>**CVE ID : CVE-2022-44171** | N/A | H-TEN-AC18-121222/752 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function R7WebsSecurityHandler.<br>**CVE ID : CVE-2022-44172** | N/A | H-TEN-AC18-121222/753 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.05 is vulnerable to Buffer Overflow via function formSetDeviceName.<br>**CVE ID : CVE-2022-44174** | N/A | H-TEN-AC18-121222/754 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetMacFilterCfg.<br>**CVE ID : CVE-2022-44175** | N/A | H-TEN-AC18-121222/755 |
| Buffer Copy without Checking Size of | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function fromSetRouteStatic. | N/A | H-TEN-AC18-121222/756 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input ('Classic Buffer Overflow') | | | **CVE ID : CVE-2022-44176** | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formWifiWpsStart.<br>**CVE ID : CVE-2022-44177** | N/A | H-TEN-AC18-121222/757 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow. via function formWifiWpsOOB.<br>**CVE ID : CVE-2022-44178** | N/A | H-TEN-AC18-121222/758 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function addWifiMacFilter.<br>**CVE ID : CVE-2022-44180** | N/A | H-TEN-AC18-121222/759 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetWifiGuestBasic.<br>**CVE ID : CVE-2022-44183** | N/A | H-TEN-AC18-121222/760 |
| **Product: ac21** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via function via set_device_name.<br>**CVE ID : CVE-2022-44158** | N/A | H-TEN-AC21-121222/761 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via function formSetMacFilterCfg.<br>**CVE ID : CVE-2022-44163** | N/A | H-TEN-AC21-121222/762 |
| **Vendor: totolink** | | | | | |
| **Product: lr350** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the FileName parameter in the UploadFirmwareFile function.<br>**CVE ID : CVE-2022-44249** | N/A | H-TOT-LR35-121222/763 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the hostName parameter in the setOpModeCfg function.<br>**CVE ID : CVE-2022-44250** | N/A | H-TOT-LR35-121222/764 |
| Improper Neutralization of | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a | N/A | H-TOT-LR35-121222/765 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Special Elements used in a Command ('Command Injection') | | | command injection via the ussd parameter in the setUssd function.<br>**CVE ID : CVE-2022-44251** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the FileName parameter in the setUploadSetting function.<br>**CVE ID : CVE-2022-44252** | N/A | H-TOT-LR35-121222/766 |
| Out-of-bounds Write | 23-Nov-2022 | 9.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a pre-authentication buffer overflow in the main function via long post data.<br>**CVE ID : CVE-2022-44255** | N/A | H-TOT-LR35-121222/767 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter ip in the setDiagnosisCfg function.<br>**CVE ID : CVE-2022-44253** | N/A | H-TOT-LR35-121222/768 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via | N/A | H-TOT-LR35-121222/769 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | parameter text in the setSmsCfg function.<br>**CVE ID : CVE-2022-44254** | | |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter pppoeUser in the setOpModeCfg function.<br>**CVE ID : CVE-2022-44257** | N/A | H-TOT-LR35-121222/770 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter command in the setTracerouteCfg function.<br>**CVE ID : CVE-2022-44258** | N/A | H-TOT-LR35-121222/771 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter week, sTime, and eTime in the setParentalRules function.<br>**CVE ID : CVE-2022-44259** | N/A | H-TOT-LR35-121222/772 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via | N/A | H-TOT-LR35-121222/773 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | parameter sPort/ePort in the setIpPortFilterRules function.<br>**CVE ID : CVE-2022-44260** | | |
| **Product: nr1800x** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter lang in the setLanguageCfg function.<br>**CVE ID : CVE-2022-44256** | N/A | H-TOT-NR18-121222/774 |
| **Vendor: ZTE** | | | | | |
| **Product: zxa10_c300m** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 22-Nov-2022 | 9.8 | There is an access control vulnerability in some ZTE PON OLT products. Due to improper access control settings, remote attackers could use the vulnerability to log in to the device and execute any operation.<br>**CVE ID : CVE-2022-39070** | https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1027824 | H-ZTE-ZXA1-121222/775 |
| **Product: zxa10_c350m** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 22-Nov-2022 | 9.8 | There is an access control vulnerability in some ZTE PON OLT | https://support.zte.com.cn/support/news | H-ZTE-ZXA1-121222/776 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | products. Due to improper access control settings, remote attackers could use the vulnerability to log in to the device and execute any operation.<br>**CVE ID : CVE-2022-39070** | /LoopholeInfoDetail.aspx?newsId=1027824 | |
| **Vendor: Zyxel** | | | | | |
| **Product: lte3301-m209** | | | | | |
| Affected Version(s): - | | | | | |
| Use of Hard-coded Credentials | 22-Nov-2022 | 9.8 | A flaw in the Zyxel LTE3301-M209 firmware verisons prior to V1.00(ABLG.6)C0 could allow a remote attacker to access the device using an improper pre-configured password if the remote administration feature has been enabled by an authenticated administrator.<br>**CVE ID : CVE-2022-40602** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-pre-configured-password-vulnerability-of-lte3301-m209 | H-ZYX-LTE3-121222/777 |
| **Operating System** | | | | | |
| **Vendor: ABB** | | | | | |
| **Product: microscada_pro_sys600** | | | | | |
| Affected Version(s): From (including) 10.0 Up to (including) 10.4 | | | | | |
| Improper Input Validation | 21-Nov-2022 | 7.8 | An input validation vulnerability exists in the Monitor Pro interface of MicroSCADA Pro and MicroSCADA X | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000123&Langu | O-ABB-MICR-121222/778 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | SYS600. An authenticated user can launch an administrator level remote code execution irrespective of the authenticated user's role.<br>**CVE ID : CVE-2022-3388** | ageCode=en&DocumentPartId=&Action=Launch&elqaid=4293&elqat=1 | |
| **Vendor: Apple** | | | | | |
| **Product: macos** | | | | | |
| Affected Version(s): - | | | | | |
| Execution with Unnecessary Privileges | 22-Nov-2022 | 7.8 | super-xray is the GUI alternative for vulnerability scanning tool xray. In 0.2-beta, a privilege escalation vulnerability was discovered. This caused inaccurate default xray permissions. Note: this vulnerability only affects Linux and Mac OS systems. Users should upgrade to super-xray 0.3-beta.<br>**CVE ID : CVE-2022-41950** | https://github.com/4ra1n/super-xray/security/advisories/GHSA-2g28-xrw6-fq5f | O-APP-MACO-121222/779 |
| **Vendor: Carel** | | | | | |
| **Product: boss_mini_firmware** | | | | | |
| Affected Version(s): 1.5.0 | | | | | |
| Incorrect Authorization | 18-Nov-2022 | 9.9 | Carel Boss Mini 1.5.0 has Improper Access Control.<br>**CVE ID : CVE-2022-34827** | N/A | O-CAR-BOSS-121222/780 |
| **Vendor: contec** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: solarview_compact_firmware** | | | | | |
| Affected Version(s): 6.00 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.8 | SolarView Compact 6.00 was discovered to contain a command injection vulnerability via network_test.php<br>**CVE ID : CVE-2022-40881** | N/A | O-CON-SOLA-121222/781 |
| **Vendor: Debian** | | | | | |
| **Product: debian_linux** | | | | | |
| Affected Version(s): 11.0 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 23-Nov-2022 | 8.8 | A logical issue in O_getOwnPropertyDescriptor() in Artifex MuJS 1.0.0 through 1.3.x before 1.3.2 allows an attacker to achieve Remote Code Execution through memory corruption, via the loading of a crafted JavaScript file.<br>**CVE ID : CVE-2022-44789** | https://github.com/alalng/CVE-2022-44789/blob/main/PublicReferenceURL.txt, https://github.com/ccxvii/mujs/commit/edb50ad66f7601ca9a3544a0e9045e8a8c60561f, https://github.com/ccxvii/mujs/releases/tag/1.3.2 | O-DEB-DEBI-121222/782 |
| **Vendor: Dlink** | | | | | |
| **Product: dir-3060_firmware** | | | | | |
| Affected Version(s): 1.11b04 | | | | | |
| Buffer Copy without Checking | 18-Nov-2022 | 9.8 | D-Link DIR3060 DIR3060A1_FW111B04.bin is vulnerable to Buffer Overflow. | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/783 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Size of Input ('Classic Buffer Overflow') | | | **CVE ID : CVE-2022-44204** | | |
| **Product: dir-823g_firmware** | | | | | |
| Affected Version(s): 1.02b03 | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 9.8 | A command injection vulnerability has been found on D-Link DIR-823G devices with firmware version 1.02B03 that allows an attacker to execute arbitrary operating system commands through well-designed /HNAP1 requests. Before the HNAP API function can process the request, the system function executes an untrusted command that triggers the vulnerability.<br>**CVE ID : CVE-2022-44808** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/784 |
| Affected Version(s): 1.02b05 | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Nov-2022 | 9.8 | D-Link DIR823G 1.02B05 is vulnerable to Commad Injection.<br>**CVE ID : CVE-2022-44201** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/785 |
| **Product: dir-878_firmware** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): 1.02b05 | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR878 1.02B04 and 1.02B05 are vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44202** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/786 |
| Improper Authentication | 22-Nov-2022 | 9.8 | D-Link DIR-878 1.02B05 is vulnerable to Incorrect Access Control.<br>**CVE ID : CVE-2022-44801** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/787 |
| Affected Version(s): 1.02b04 | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR878 1.02B04 and 1.02B05 are vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44202** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/788 |
| **Product: dir-882_firmware** | | | | | |
| Affected Version(s): 1.10b02 | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and1.20B06 is vulnerable to Buffer Overflow via the websRedirect function.<br>**CVE ID : CVE-2022-44804** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/789 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44806** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/790 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer | https://www.dlink.com/en | O-DLI-DIR--121222/791 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Overflow via webGetVarString.<br>**CVE ID : CVE-2022-44807** | /security-bulletin/ | |
| Affected Version(s): 1.20b06 | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and1.20B06 is vulnerable to Buffer Overflow via the websRedirect function.<br>**CVE ID : CVE-2022-44804** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/792 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow.<br>**CVE ID : CVE-2022-44806** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/793 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | D-Link DIR-882 1.10B02 and 1.20B06 is vulnerable to Buffer Overflow via webGetVarString.<br>**CVE ID : CVE-2022-44807** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--121222/794 |
| **Product: dsl-224_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 17-Nov-2022 | 9.9 | DLINK - DSL-224 Post-auth PCE. DLINK router has an interface where you can configure NTP servers (Network Time Protocol) via jsonrpc API. It is possible to inject a command through this interface that will run with | N/A | O-DLI-DSL--121222/795 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ROOT permissions on the router.<br>**CVE ID : CVE-2022-36786** | | |
| **Product: g_integrated_access_device4_firmware** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Incorrect Authorization | 17-Nov-2022 | 7.5 | D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass. *Information Disclosure – file contains a URL with private IP at line 15 "login.asp" A. The window.location.href = http://192.168.1.1/setupWizard.asp" http://192.168.1.1/setupWizard.asp" ; "admin" – contains default username value "login.asp" B. While accessing the web interface, the login form at *Authorization Bypass – URL by "setupWizard.asp' while it blocks direct access to – the web interface does not properly validate user identity variables values located at the client side, it is available to access it without a "login_glag" and "login_status" checking browser and to read the admin user | N/A | O-DLI-G_IN-121222/796 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | credentials for the web interface.<br>**CVE ID : CVE-2022-36785** | | |
| **Vendor: elsight** | | | | | |
| **Product: halo_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 17-Nov-2022 | 9.8 | Elsight – Elsight Halo Remote Code Execution (RCE) Elsight Halo web panel allows us to perform connection validation. through the POST request : /api/v1/nics/wifi/wlan0/ping we can abuse DESTINATION parameter and leverage it to remote code execution.<br>**CVE ID : CVE-2022-36784** | N/A | O-ELS-HALO-121222/797 |
| **Vendor: Fedoraproject** | | | | | |
| **Product: fedora** | | | | | |
| Affected Version(s): 35 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 6.1 | A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in | http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76091, https://moodle.org/mod/forum/discuss.php?d=440770 | O-FED-FEDO-121222/798 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.<br>**CVE ID : CVE-2022-45150** |  |  |
| Cross-Site Request Forgery (CSRF) | 23-Nov-2022 | 5.4 | A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.<br>**CVE ID : CVE-2022-45149** | https://moodle.org/mod/forum/discuss.php?d=440769, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75862 | O-FED-FEDO-121222/799 |
| Improper Neutralization of | 23-Nov-2022 | 5.4 | The stored-XSS vulnerability was discovered in Moodle | https://moodle.org/mod/forum/discuss.p | O-FED-FEDO-121222/800 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input During Web Page Generation ('Cross-site Scripting') | | | which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.<br>**CVE ID : CVE-2022-45151** | hp?d=440771, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76131 | |
| Affected Version(s): 36 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 6.1 | A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages. | http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76091, https://moodle.org/mod/forum/discuss.php?d=440770 | O-FED-FEDO-121222/801 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-45150** | | |
| Cross-Site Request Forgery (CSRF) | 23-Nov-2022 | 5.4 | A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.<br>**CVE ID : CVE-2022-45149** | https://moodle.org/mod/forum/discuss.php?d=440769, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75862 | O-FED-FEDO-121222/802 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 5.4 | The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in | https://moodle.org/mod/forum/discuss.php?d=440771, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76131 | O-FED-FEDO-121222/803 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | context of vulnerable website.<br>**CVE ID : CVE-2022-45151** | | |
| Uncaught Exception | 22-Nov-2022 | 5.1 | A vulnerability was found in keylime. This security issue happens in some circumstances, due to some improperly handled exceptions, there exists the possibility that a rogue agent could create errors on the verifier that stopped attestation attempts for that host leaving it in an attested state but not verifying that anymore.<br>**CVE ID : CVE-2022-3500** | https://github.com/keylime/keylime/pull/1128 | O-FED-FEDO-121222/804 |
| Affected Version(s): 37 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Nov-2022 | 6.1 | A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may | http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76091,<br>https://moodle.org/mod/forum/discuss.php?d=440770 | O-FED-FEDO-121222/805 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.<br>**CVE ID : CVE-2022-45150** | | |
| Cross-Site Request Forgery (CSRF) | 23-Nov-2022 | 5.4 | A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.<br>**CVE ID : CVE-2022-45149** | https://moodle.org/mod/forum/discuss.php?d=440769, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75862 | O-FED-FEDO-121222/806 |
| Improper Neutralization of Input During Web Page | 23-Nov-2022 | 5.4 | The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user- | https://moodle.org/mod/forum/discuss.php?d=440771, http://git.moodle.org/gw? | O-FED-FEDO-121222/807 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.<br>**CVE ID : CVE-2022-45151** | p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76131 | |
| **Vendor: Google** | | | | | |
| **Product: android** | | | | | |
| Affected Version(s): - | | | | | |
| Integer Overflow or Wraparound | 17-Nov-2022 | 7.8 | In shared_metadata_init of SharedMetadata.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239415718References: N/A<br>**CVE ID : CVE-2022-42533** | https://source.android.com/security/bulletin/pixel/2022-11-01 | O-GOO-ANDR-121222/808 |
| Out-of-bounds Write | 17-Nov-2022 | 6.7 | In (TBD) of (TBD), there is a possible way to corrupt memory due to improper input validation. This could lead to local escalation | https://source.android.com/security/bulletin/pixel/2022-11-01 | O-GOO-ANDR-121222/809 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239555070References: N/A<br>**CVE ID : CVE-2022-20427** |  |  |
| Out-of-bounds Write | 17-Nov-2022 | 6.7 | In (TBD) of (TBD), 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-239555411References: N/A<br>**CVE ID : CVE-2022-20428** | https://source.android.com/security/bulletin/pixel/2022-11-01 | O-GOO-ANDR-121222/810 |
| Improper Input Validation | 17-Nov-2022 | 6.7 | In (TBD) of (TBD), there is a possible way to redirect code execution due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not | https://source.android.com/security/bulletin/pixel/2022-11-01 | O-GOO-ANDR-121222/811 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239556260References : N/A<br>**CVE ID : CVE-2022-20459** | | |
| Out-of-bounds Write | 17-Nov-2022 | 6.7 | In (TBD) mprot_unmap? of (TBD), there is a possible way to corrupt the memory mapping due to improper input validation. 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-239557547References : N/A<br>**CVE ID : CVE-2022-20460** | https://source.android.com/security/bulletin/pixel/2022-11-01 | O-GOO-ANDR-121222/812 |
| **Vendor: IBM** | | | | | |
| **Product: aix** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Comman | 16-Nov-2022 | 9.8 | IBM InfoSphere DataStage 11.7 is vulnerable to a command injection vulnerability due to improper neutralization of | https://www.ibm.com/support/pages/node/6833566, https://exchange.xforce.ibmcloud.com/v | O-IBM-AIX-121222/813 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| d Injection') | | | special elements. IBM X-Force ID: 236687.<br>**CVE ID : CVE-2022-40752** | ulnerabilities/236687 | |
| **Vendor: intelbras** | | | | | |
| **Product: sg_2404_mr_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Privilege Management | 18-Nov-2022 | 7.8 | INTELBRAS SG 2404 MR 20180928-rel64938 allows authenticated attackers to arbitrarily create Administrator accounts via crafted user cookies.<br>**CVE ID : CVE-2022-43308** | N/A | O-INT-SG_2-121222/814 |
| **Product: sg_2404_poe_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Privilege Management | 18-Nov-2022 | 7.8 | INTELBRAS SG 2404 MR 20180928-rel64938 allows authenticated attackers to arbitrarily create Administrator accounts via crafted user cookies.<br>**CVE ID : CVE-2022-43308** | N/A | O-INT-SG_2-121222/815 |
| **Vendor: Linux** | | | | | |
| **Product: linux_kernel** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in a Command | 16-Nov-2022 | 9.8 | IBM InfoSphere DataStage 11.7 is vulnerable to a command injection vulnerability due to improper neutralization of | https://www.ibm.com/support/pages/node/6833566, https://exchange.xforce.ibmcloud.com/v | O-LIN-LINU-121222/816 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Command Injection') | | | special elements. IBM X-Force ID: 236687.<br>**CVE ID : CVE-2022-40752** | ulnerabilities/236687 | |
| Use After Free | 23-Nov-2022 | 8.8 | There are use-after-free vulnerabilities in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_connect and l2cap_le_connect_req functions which may allow code execution and leaking kernel memory (respectively) remotely via Bluetooth. A remote attacker could execute code leaking kernel memory via Bluetooth if within proximity of the victim. We recommend upgrading past commit https://www.google.com/url https://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4 https://www.google.com/url<br>**CVE ID : CVE-2022-42896** | https://kernel.dance/#711f8c3fb3db61897080468586b970c87c61d9e4, https://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4 | O-LIN-LINU-121222/817 |
| Improper Neutralization of Special Elements used in an | 17-Nov-2022 | 8.8 | The Java Admin Console in Veritas NetBackup through 10.1 and related Veritas products on Linux and UNIX allows | https://www.veritas.com/content/support/en_US/sec | O-LIN-LINU-121222/818 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| OS Command ('OS Command Injection') | | | authenticated non-root users (that have been explicitly added to the auth.conf file) to execute arbitrary commands as root.<br>**CVE ID : CVE-2022-45461** | urity/VTS22-015 | |
| Improper Input Validation | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer (nvidia.ko), where a local user with basic capabilities can cause improper input validation, which may lead to denial of service, escalation of privileges, data tampering, and limited information disclosure.<br>**CVE ID : CVE-2022-31607** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-LIN-LINU-121222/819 |
| Execution with Unnecessary Privileges | 22-Nov-2022 | 7.8 | super-xray is the GUI alternative for vulnerability scanning tool xray. In 0.2-beta, a privilege escalation vulnerability was discovered. This caused inaccurate default xray permissions. Note: this vulnerability only affects Linux and Mac OS systems. Users should upgrade to super-xray 0.3-beta. | https://github.com/4ra1n/super-xray/security/advisories/GHSA-2g28-xrw6-fq5f | O-LIN-LINU-121222/820 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-41950** | | |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-LIN-LINU-121222/821 |
| Access of Uninitialized Pointer | 23-Nov-2022 | 5.5 | There is an infoleak vulnerability in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_parse_conf_req function which can be used to leak kernel pointers remotely. We recommend upgrading past commit https://github.com/torvalds/linux/commit/b1a2cd50c0357f243b7435a732b4e62ba3157a2e https://www.google.com/url<br>**CVE ID : CVE-2022-42895** | https://kernel.dance/#b1a2cd50c0357f243b7435a732b4e62ba3157a2e, https://github.com/torvalds/linux/commit/b1a2cd50c0357f243b7435a732b4e62ba3157a2e | O-LIN-LINU-121222/822 |
| Insecure Storage of Sensitive Information | 16-Nov-2022 | 3.3 | IBM Sterling Partner Engagement Manager 2.0 allows encrypted storage of client data to be stored locally which can be read by | https://www.ibm.com/support/pages/node/6839751, https://exchange.xforce.ib | O-LIN-LINU-121222/823 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | another user on the system. IBM X-Force ID: 230424.<br>**CVE ID : CVE-2022-34354** | mcloud.com/vulnerabilities/230424 | |
| Affected Version(s): * Up to (excluding) 6.0 | | | | | |
| Use After Free | 22-Nov-2022 | 7.8 | Use After Free vulnerability in Linux Kernel allows Privilege Escalation. An improper Update of Reference Count in io_uring leads to Use-After-Free and Local Privilege Escalation. When io_msg_ring was invoked with a fixed file, it called io_fput_file() which improperly decreased its reference count (leading to Use-After-Free and Local Privilege Escalation). Fixed files are permanently registered to the ring, and should not be put separately. We recommend upgrading past commit https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679 https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679 | https://kernel.dance/#fc7222c3a9f56271fba02aabbfbae999042f1679,<br>https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679 | O-LIN-LINU-121222/824 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-3910** | | |
| Affected Version(s): * Up to (including) 6.0.10 | | | | | |
| Use After Free | 27-Nov-2022 | 7 | An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait_event.<br>**CVE ID : CVE-2022-45919** | https://lore.kernel.org/linux-media/20221121063308.GA33821@ubuntu/T/#u | O-LIN-LINU-121222/825 |
| Affected Version(s): * Up to (including) 6.0.9 | | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 25-Nov-2022 | 7 | An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops.<br>**CVE ID : CVE-2022-45884** | https://lore.kernel.org/linux-media/20221115131822.6640-4-imv4bel@gmail.com/,<br>https://lore.kernel.org/linux-media/20221115131822.6640-1-imv4bel@gmail.com/ | O-LIN-LINU-121222/826 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 25-Nov-2022 | 7 | An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_frontend.c has a race condition that can cause a use-after-free when a | https://lore.kernel.org/linux-media/20221115131822.6640-2-imv4bel@gmail.com/,<br>https://lore.k | O-LIN-LINU-121222/827 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | device is disconnected.<br>**CVE ID : CVE-2022-45885** | ernel.org/linux-media/20221115131822.6640-1-imv4bel@gmail.com/ | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 25-Nov-2022 | 7 | An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect versus dvb_device_open race condition that leads to a use-after-free.<br>**CVE ID : CVE-2022-45886** | https://lore.kernel.org/linux-media/20221115131822.6640-3-imv4bel@gmail.com/, https://lore.kernel.org/linux-media/20221115131822.6640-1-imv4bel@gmail.com/ | O-LIN-LINU-121222/828 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 25-Nov-2022 | 6.4 | An issue was discovered in the Linux kernel through 6.0.9. drivers/char/xillybus/xillyusb.c has a race condition and use-after-free during physical removal of a USB device.<br>**CVE ID : CVE-2022-45888** | https://lore.kernel.org/all/20221022175404.GA375335@ubuntu/ | O-LIN-LINU-121222/829 |
| Concurrent Execution using Shared Resource with Improper Synchroniz | 25-Nov-2022 | 4.7 | An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak because of the lack of | https://lore.kernel.org/linux-media/20221115131822.6640-5-imv4bel@gmail.com/, | O-LIN-LINU-121222/830 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ation ('Race Condition') | | | a dvb_frontend_detach call.<br>**CVE ID : CVE-2022-45887** | https://lore.kernel.org/linux-media/20221115131822.6640-1-imv4bel@gmail.com/ | |
| Affected Version(s): 6.0 | | | | | |
| Use After Free | 22-Nov-2022 | 7.8 | Use After Free vulnerability in Linux Kernel allows Privilege Escalation. An improper Update of Reference Count in io_uring leads to Use-After-Free and Local Privilege Escalation. When io_msg_ring was invoked with a fixed file, it called io_fput_file() which improperly decreased its reference count (leading to Use-After-Free and Local Privilege Escalation). Fixed files are permanently registered to the ring, and should not be put separately. We recommend upgrading past commit https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679<br>https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba | https://kernel.dance/#fc7222c3a9f56271fba02aabbfbae999042f1679, https://github.com/torvalds/linux/commit/fc7222c3a9f56271fba02aabbfbae999042f1679 | O-LIN-LINU-121222/831 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | 02aabbfbae999042f1679<br>**CVE ID : CVE-2022-3910** |  |  |
| **Vendor: m5t** |  |  |  |  |  |
| **Product: mediatrix_4102s_firmware** |  |  |  |  |  |
| Affected Version(s): * Up to (excluding) 48.5.2718 |  |  |  |  |  |
| N/A | 17-Nov-2022 | 6.8 | Mediatrix 4102 before v48.5.2718 allows local attackers to gain root access via the UART port.<br>**CVE ID : CVE-2022-43096** | https://documentation.media5corp.com/display/MP/DGW+Security+Improvement+Notes+v48.5.2718 | O-M5T-MEDI-121222/832 |
| **Vendor: Microsoft** |  |  |  |  |  |
| **Product: windows** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 16-Nov-2022 | 9.8 | IBM InfoSphere DataStage 11.7 is vulnerable to a command injection vulnerability due to improper neutralization of special elements. IBM X-Force ID: 236687.<br>**CVE ID : CVE-2022-40752** | https://www.ibm.com/support/pages/node/6833566, https://exchange.xforce.ibmcloud.com/vulnerabilities/236687 | O-MIC-WIND-121222/833 |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a failure to properly validate data might allow an | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/834 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker with basic user capabilities to cause an out-of-bounds access in kernel mode, which could lead to denial of service, information disclosure, escalation of privileges, or data tampering.<br>**CVE ID : CVE-2022-31606** | | |
| Out-of-bounds Write | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds write, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31610** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/835 |
| Out-of-bounds Read | 19-Nov-2022 | 7.8 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a local user with basic capabilities can cause an out-of-bounds read, which may lead to code execution, denial of | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/836 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | service, escalation of privileges, information disclosure, or data tampering.<br>**CVE ID : CVE-2022-31617** | | |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to a system crash or a leak of internal kernel information.<br>**CVE ID : CVE-2022-31612** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/837 |
| Out-of-bounds Read | 19-Nov-2022 | 7.1 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where a local user with basic capabilities can cause an out-of-bounds read, which may lead to denial of service, or information disclosure. | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/838 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-31616** | | |
| Uncontrolled Search Path Element | 21-Nov-2022 | 6.7 | IBM i Access Family 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236581.<br>**CVE ID : CVE-2022-40746** | https://exchange.xforce.ibmcloud.com/vulnerabilities/236581, https://www.ibm.com/support/pages/node/6840359 | O-MIC-WIND-121222/839 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where any local user can cause a null-pointer dereference, which may lead to a kernel panic.<br>**CVE ID : CVE-2022-31613** | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/840 |
| NULL Pointer Dereference | 19-Nov-2022 | 6.5 | NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities | https://nvidia.custhelp.com/app/answers/detail/a_id/5383 | O-MIC-WIND-121222/841 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | can cause a null-pointer dereference, which may lead to denial of service.<br>**CVE ID : CVE-2022-34665** | | |
| Out-of-bounds Write | 19-Nov-2022 | 4.4 | NVIDIA CUDA Toolkit SDK contains a stack-based buffer overflow vulnerability in cuobjdump, where an unprivileged remote attacker could exploit this buffer overflow condition by persuading a local user to download a specially crafted corrupted file and execute cuobjdump against it locally, which may lead to a limited denial of service and some loss of data integrity for the local user.<br>**CVE ID : CVE-2022-34667** | https://nvidia.custhelp.com/app/answers/detail/a_id/5373 | O-MIC-WIND-121222/842 |
| **Vendor: Netgear** | | | | | |
| **Product: r7000p_firmware** | | | | | |
| Affected Version(s): 1.3.0.8 | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter wan_dns1_sec.<br>**CVE ID : CVE-2022-44184** | https://www.netgear.com/about/security/ | O-NET-R700-121222/843 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via wan_dns1_pri.<br>**CVE ID : CVE-2022-44187** | https://www.netgear.com/about/security/ | O-NET-R700-121222/844 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter enable_band_steering.<br>**CVE ID : CVE-2022-44188** | https://www.netgear.com/about/security/ | O-NET-R700-121222/845 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameters apmode_dns1_pri and apmode_dns1_sec.<br>**CVE ID : CVE-2022-44194** | http://netgear.com, https://www.netgear.com/about/security/ | O-NET-R700-121222/846 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameter openvpn_push1.<br>**CVE ID : CVE-2022-44196** | https://www.netgear.com/about/security/ | O-NET-R700-121222/847 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameter openvpn_server_ip.<br>**CVE ID : CVE-2022-44197** | https://www.netgear.com/about/security/ | O-NET-R700-121222/848 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8, V1.3.1.64 is vulnerable to Buffer Overflow via parameters: | https://www.netgear.com/about/security/ | O-NET-R700-121222/849 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | stamode_dns1_pri and stamode_dns1_sec.<br>**CVE ID : CVE-2022-44200** | | |
| Affected Version(s): 1.3.1.64 | | | | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameter wan_dns1_pri.<br>**CVE ID : CVE-2022-44186** | https://www.netgear.com/about/security/ | O-NET-R700-121222/850 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter enable_band_steering.<br>**CVE ID : CVE-2022-44190** | https://www.netgear.com/about/security/ | O-NET-R700-121222/851 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameters KEY1 and KEY2.<br>**CVE ID : CVE-2022-44191** | https://www.netgear.com/about/security/ | O-NET-R700-121222/852 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow in /usr/sbin/httpd via parameters: starthour, startminute , endhour, and endminute.<br>**CVE ID : CVE-2022-44193** | https://www.netgear.com/about/security/ | O-NET-R700-121222/853 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via | https://www.netgear.com/about/security/ | O-NET-R700-121222/854 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | parameter openvpn_push1.<br>**CVE ID : CVE-2022-44198** | | |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.1.64 is vulnerable to Buffer Overflow via parameter openvpn_server_ip.<br>**CVE ID : CVE-2022-44199** | https://www.netgear.com/about/security/ | O-NET-R700-121222/855 |
| Out-of-bounds Write | 22-Nov-2022 | 9.8 | Netgear R7000P V1.3.0.8, V1.3.1.64 is vulnerable to Buffer Overflow via parameters: stamode_dns1_pri and stamode_dns1_sec.<br>**CVE ID : CVE-2022-44200** | https://www.netgear.com/about/security/ | O-NET-R700-121222/856 |
| **Vendor: nxp** | | | | | |
| **Product: i.mx_6duallite_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents | N/A | O-NXP-I.MX-121222/857 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6dualplus_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm | N/A | O-NXP-I.MX-121222/858 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6dual_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by | N/A | O-NXP-I.MX-121222/859 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6quadplus_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for | N/A | O-NXP-I.MX-121222/860 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_6quad_firmware** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | O-NXP-I.MX-121222/861 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: i.mx_6sololite_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | O-NXP-I.MX-121222/862 |
| **Product: i.mx_6solox_firmware** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | O-NXP-I.MX-121222/863 |
| **Product: i.mx_6solo_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in | N/A | O-NXP-I.MX-121222/864 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6ull_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT | N/A | O-NXP-I.MX-121222/865 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6ultralite_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device | N/A | O-NXP-I.MX-121222/866 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_6ulz_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically | N/A | O-NXP-I.MX-121222/867 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_6_firmware** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended | N/A | O-NXP-I.MX-121222/868 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_7dual_firmware** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable | N/A | O-NXP-I.MX-121222/869 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_7solo_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.) | N/A | O-NXP-I.MX-121222/870 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_7ulp_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | O-NXP-I.MX-121222/871 |
| **Product: i.mx_8m_mini_firmware** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | N/A | O-NXP-I.MX-121222/872 |
| **Product: i.mx_8m_quad_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in | N/A | O-NXP-I.MX-121222/873 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_8m_vybrid_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT | N/A | O-NXP-I.MX-121222/874 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_rt1010_firmware** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device | N/A | O-NXP-I.MX-121222/875 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1015_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically | N/A | O-NXP-I.MX-121222/876 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1020_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended | N/A | O-NXP-I.MX-121222/877 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** |  |  |
| **Product: i.mx_rt1050_firmware** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable | N/A | O-NXP-I.MX-121222/878 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | eFUSE. Customers can contact NXP for additional information.)<br>**CVE ID : CVE-2022-45163** | | |
| **Product: i.mx_rt1060_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Observable Discrepancy | 18-Nov-2022 | 4.6 | An information-disclosure vulnerability exists on select NXP devices when configured in Serial Download Protocol (SDP) mode: i.MX RT 1010, i.MX RT 1015, i.MX RT 1020, i.MX RT 1050, i.MX RT 1060, i.MX 6 Family, i.MX 7Dual/Solo, i.MX 7ULP, i.MX 8M Quad, i.MX 8M Mini, and Vybrid. In a device security-enabled configuration, memory contents could potentially leak to physically proximate attackers via the respective SDP port in cold and warm boot attacks. (The recommended mitigation is to completely disable the SDP mode by programming a one-time programmable eFUSE. Customers can contact NXP for additional information.) | N/A | O-NXP-I.MX-121222/879 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | **CVE ID : CVE-2022-45163** |  |  |
| **Vendor: opengroup** |  |  |  |  |  |
| **Product: unix** |  |  |  |  |  |
| Affected Version(s): - |  |  |  |  |  |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 17-Nov-2022 | 8.8 | The Java Admin Console in Veritas NetBackup through 10.1 and related Veritas products on Linux and UNIX allows authenticated non-root users (that have been explicitly added to the auth.conf file) to execute arbitrary commands as root.<br>**CVE ID : CVE-2022-45461** | https://www.veritas.com/content/support/en_US/security/VTS22-015 | O-OPE-UNIX-121222/880 |
| **Vendor: Realtek** |  |  |  |  |  |
| **Product: rtl8111ep-cg_firmware** |  |  |  |  |  |
| Affected Version(s): * Up to (including) 3.0.0.2019090 |  |  |  |  |  |
| Use of Hard-coded Credentials | 29-Nov-2022 | 2.1 | RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated physical attacker can use the hard-coded default password during system reboot triggered by other user, to acquire partial system information such as serial number and server information.<br>**CVE ID : CVE-2022-32967** | N/A | O-REA-RTL8-121222/881 |
| Affected Version(s): 5.0.10 |  |  |  |  |  |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Hard-coded Credentials | 29-Nov-2022 | 2.1 | RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated physical attacker can use the hard-coded default password during system reboot triggered by other user, to acquire partial system information such as serial number and server information.<br>**CVE ID : CVE-2022-32967** | N/A | O-REA-RTL8-121222/882 |
| **Product: rtl8111fp-cg_firmware** | | | | | |
| Affected Version(s): * Up to (including) 3.0.0.2019090 | | | | | |
| Use of Hard-coded Credentials | 29-Nov-2022 | 2.1 | RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated physical attacker can use the hard-coded default password during system reboot triggered by other user, to acquire partial system information such as serial number and server information.<br>**CVE ID : CVE-2022-32967** | N/A | O-REA-RTL8-121222/883 |
| Affected Version(s): 5.0.10 | | | | | |
| Use of Hard-coded Credentials | 29-Nov-2022 | 2.1 | RTL8111EP-CG/RTL8111FP-CG DASH function has hard-coded password. An unauthenticated | N/A | O-REA-RTL8-121222/884 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | physical attacker can use the hard-coded default password during system reboot triggered by other user, to acquire partial system information such as serial number and server information.<br>**CVE ID : CVE-2022-32967** | | |
| Affected Version(s): * Up to (including) 5.0.23 | | | | | |
| Missing Authorization | 29-Nov-2022 | 6.5 | RTL8168FP-CG Dash remote management function has missing authorization. An unauthenticated attacker within the adjacent network can connect to DASH service port to disrupt service.<br>**CVE ID : CVE-2022-32966** | N/A | O-REA-RTL8-121222/885 |
| **Vendor: Redhat** | | | | | |
| **Product: enterprise_linux** | | | | | |
| Affected Version(s): 9.0 | | | | | |
| Uncaught Exception | 22-Nov-2022 | 5.1 | A vulnerability was found in keylime. This security issue happens in some circumstances, due to some improperly handled exceptions, there exists the possibility that a rogue agent could create errors on the verifier that stopped attestation attempts | https://github.com/keylime/keylime/pull/1128 | O-RED-ENTE-121222/886 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | for that host leaving it in an attested state but not verifying that anymore.<br>**CVE ID : CVE-2022-3500** | | |
| **Vendor: Tenda** | | | | | |
| **Product: ac15_firmware** | | | | | |
| Affected Version(s): 15.03.05.18 | | | | | |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.18 is avulnerable to Buffer Overflow via function formSetPPTPServer.<br>**CVE ID : CVE-2022-44167** | N/A | O-TEN-AC15-121222/887 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.18 is vulnerable to Buffer Overflow via function fromSetRouteStatic..<br>**CVE ID : CVE-2022-44168** | N/A | O-TEN-AC15-121222/888 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.18 is vulnerable to Buffer Overflow via function formSetVirtualSer.<br>**CVE ID : CVE-2022-44169** | N/A | O-TEN-AC15-121222/889 |
| Affected Version(s): 15.03.05.19 | | | | | |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC15 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetIpMacBind.<br>**CVE ID : CVE-2022-44156** | N/A | O-TEN-AC15-121222/890 |
| **Product: ac18_firmware** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): 15.03.05.19 | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function form_fast_setting_wifi_set.<br>**CVE ID : CVE-2022-44171** | N/A | O-TEN-AC18-121222/891 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function R7WebsSecurityHandler.<br>**CVE ID : CVE-2022-44172** | N/A | O-TEN-AC18-121222/892 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetMacFilterCfg.<br>**CVE ID : CVE-2022-44175** | N/A | O-TEN-AC18-121222/893 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function fromSetRouteStatic.<br>**CVE ID : CVE-2022-44176** | N/A | O-TEN-AC18-121222/894 |
| Buffer Copy without Checking Size of | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formWifiWpsStart. | N/A | O-TEN-AC18-121222/895 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input ('Classic Buffer Overflow') | | | **CVE ID : CVE-2022-44177** | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow. via function formWifiWpsOOB.<br>**CVE ID : CVE-2022-44178** | N/A | O-TEN-AC18-121222/896 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function addWifiMacFilter.<br>**CVE ID : CVE-2022-44180** | N/A | O-TEN-AC18-121222/897 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via function formSetWifiGuestBasic.<br>**CVE ID : CVE-2022-44183** | N/A | O-TEN-AC18-121222/898 |
| Affected Version(s): 15.03.05.05 | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 21-Nov-2022 | 9.8 | Tenda AC18 V15.03.05.05 is vulnerable to Buffer Overflow via function formSetDeviceName.<br>**CVE ID : CVE-2022-44174** | N/A | O-TEN-AC18-121222/899 |
| **Product: ac21_firmware** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): 16.03.08.15 | | | | | |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via function via set_device_name.<br>**CVE ID : CVE-2022-44158** | N/A | O-TEN-AC21-121222/900 |
| Out-of-bounds Write | 21-Nov-2022 | 7.5 | Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via function formSetMacFilterCfg.<br>**CVE ID : CVE-2022-44163** | N/A | O-TEN-AC21-121222/901 |
| **Vendor: totolink** | | | | | |
| **Product: lr350_firmware** | | | | | |
| Affected Version(s): 9.3.5u.6369_b20220309 | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the FileName parameter in the UploadFirmwareFile function.<br>**CVE ID : CVE-2022-44249** | N/A | O-TOT-LR35-121222/902 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the hostName parameter in the setOpModeCfg function.<br>**CVE ID : CVE-2022-44250** | N/A | O-TOT-LR35-121222/903 |
| Improper Neutralizat | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210 | N/A | O-TOT-LR35-121222/904 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ion of Special Elements used in a Command ('Command Injection') | | | 910 contains a command injection via the ussd parameter in the setUssd function.<br>**CVE ID : CVE-2022-44251** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Nov-2022 | 9.8 | TOTOLINK NR1800X V9.1.0u.6279_B20210910 contains a command injection via the FileName parameter in the setUploadSetting function.<br>**CVE ID : CVE-2022-44252** | N/A | O-TOT-LR35-121222/905 |
| Out-of-bounds Write | 23-Nov-2022 | 9.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a pre-authentication buffer overflow in the main function via long post data.<br>**CVE ID : CVE-2022-44255** | N/A | O-TOT-LR35-121222/906 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter ip in the setDiagnosisCfg function.<br>**CVE ID : CVE-2022-44253** | N/A | O-TOT-LR35-121222/907 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via | N/A | O-TOT-LR35-121222/908 |

| CVSS Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|---|---|---|

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | parameter text in the setSmsCfg function.<br>**CVE ID : CVE-2022-44254** |  |  |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter pppoeUser in the setOpModeCfg function.<br>**CVE ID : CVE-2022-44257** | N/A | O-TOT-LR35-121222/909 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter command in the setTracerouteCfg function.<br>**CVE ID : CVE-2022-44258** | N/A | O-TOT-LR35-121222/910 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter week, sTime, and eTime in the setParentalRules function.<br>**CVE ID : CVE-2022-44259** | N/A | O-TOT-LR35-121222/911 |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via | N/A | O-TOT-LR35-121222/912 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | parameter sPort/ePort in the setIpPortFilterRules function.<br>**CVE ID : CVE-2022-44260** | | |
| **Product: nr1800x_firmware** | | | | | |
| Affected Version(s): 9.3.5u.6369_b20220309 | | | | | |
| Out-of-bounds Write | 23-Nov-2022 | 8.8 | TOTOLINK LR350 V9.3.5u.6369_B20220309 contains a post-authentication buffer overflow via parameter lang in the setLanguageCfg function.<br>**CVE ID : CVE-2022-44256** | N/A | O-TOT-NR18-121222/913 |
| **Vendor: ZTE** | | | | | |
| **Product: zxa10_c300m_firmware** | | | | | |
| Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.1.0xgp002.4 | | | | | |
| N/A | 22-Nov-2022 | 9.8 | There is an access control vulnerability in some ZTE PON OLT products. Due to improper access control settings, remote attackers could use the vulnerability to log in to the device and execute any operation.<br>**CVE ID : CVE-2022-39070** | https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1027824 | O-ZTE-ZXA1-121222/914 |
| **Product: zxa10_c350m_firmware** | | | | | |
| Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.1.0xgp002.4 | | | | | |
| N/A | 22-Nov-2022 | 9.8 | There is an access control vulnerability in some ZTE PON OLT | https://support.zte.com.cn/support/news | O-ZTE-ZXA1-121222/915 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | products. Due to improper access control settings, remote attackers could use the vulnerability to log in to the device and execute any operation.<br>**CVE ID : CVE-2022-39070** | /LoopholeInfoDetail.aspx?newsId=1027824 | |
| **Vendor: Zyxel** | | | | | |
| **Product: lte3301-m209_firmware** | | | | | |
| Affected Version(s): * Up to (excluding) 1.00\\(ablg.6\\)c0 | | | | | |
| Use of Hard-coded Credentials | 22-Nov-2022 | 9.8 | A flaw in the Zyxel LTE3301-M209 firmware verisons prior to V1.00(ABLG.6)C0 could allow a remote attacker to access the device using an improper pre-configured password if the remote administration feature has been enabled by an authenticated administrator.<br>**CVE ID : CVE-2022-40602** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-pre-configured-password-vulnerability-of-lte3301-m209 | O-ZYX-LTE3-121222/916 |