https://nciipc.gov.in

# National Critical Information Infrastructure Protection Centre

# Common Vulnerabilities and Exposures(CVE) Report

**16 - 28 Feb 2021 Vol. 08 No. 04**

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Accellion** | | | | | |
| **fta** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Feb-21 | 7.5 | Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html. The fixed version is FTA_9_12_380 and later.<br>**CVE ID : CVE-2021-27101** | https://www.accellion.com/products/fta/ | A-ACC-FTA-020321/1 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 16-Feb-21 | 7.2 | Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call. The fixed version is FTA_9_12_416 and later.<br>**CVE ID : CVE-2021-27102** | https://www.accellion.com/products/fta/ | A-ACC-FTA-020321/2 |
| Server-Side Request Forgery (SSRF) | 16-Feb-21 | 7.5 | Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html. The fixed version is FTA_9_12_416 and later.<br>**CVE ID : CVE-2021-27103** | https://www.accellion.com/products/fta/ | A-ACC-FTA-020321/3 |
| Improper Neutralization of Special Elements used in an OS Command | 16-Feb-21 | 10 | Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints. The fixed version is | https://www.accellion.com/products/fta/ | A-ACC-FTA-020321/4 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('OS Command Injection') | |  | FTA_9_12_380 and later.<br>**CVE ID : CVE-2021-27104** | | |
| **Adobe** | | | | | |
| **bridge** | | | | | |
| Out-of-bounds Write | 25-Feb-21 | 6.8 | Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2021-21065** | https://helpx.adobe.com/security/products/bridge/apsb21-07.html | A-ADO-BRID-020321/5 |
| Out-of-bounds Write | 25-Feb-21 | 6.8 | Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2021-21066** | https://helpx.adobe.com/security/products/bridge/apsb21-07.html | A-ADO-BRID-020321/6 |
| **Apache** | | | | | |
| **airflow** | | | | | |
| Improper Privilege Management | 17-Feb-21 | 4 | Improper Access Control on Configurations Endpoint for the Stable API of Apache Airflow allows users with Viewer or User role to get Airflow Configurations including sensitive | https://lists.apache.org/thread.html/r3b3787700279ec361308cbefb7c2cce2acb26891a | A-APA-AIRF-020321/7 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information even when `[webserver] expose_config` is set to `False` in `airflow.cfg`. This allowed a privilege escalation attack. This issue affects Apache Airflow 2.0.0.<br>**CVE ID : CVE-2021-26559** | 12ce864e4a13c8d%40%3Cusers.airflow.apache.org%3E, https://lists.apache.org/thread.html/rd142565996d7ee847b9c14b8a9921dcf80bc6bc160e3d9dca6dfc2f8@%3Cannounce.apache.org%3E | |
| Improper Authentication | 17-Feb-21 | 5 | The lineage endpoint of the deprecated Experimental API was not protected by authentication in Airflow 2.0.0. This allowed unauthenticated users to hit that endpoint. This is low-severity issue as the attacker needs to be aware of certain parameters to pass to that endpoint and even after can just get some metadata about a DAG and a Task. This issue affects Apache Airflow 2.0.0.<br>**CVE ID : CVE-2021-26697** | N/A | A-APA-AIRF-020321/8 |
| **myfaces** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 6.8 | In the default configuration, Apache MyFaces Core versions 2.2.0 to 2.2.13, 2.3.0 to 2.3.7, 2.3-next-M1 to 2.3-next-M4, and 3.0.0-RC1 use cryptographically weak implicit and explicit cross-site request forgery (CSRF) | https://lists.apache.org/thread.html/r2b73e2356c6155e9ec78fdd8f72a4fac12f3e588014f5f535106e | A-APA-MYFA-020321/9 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | tokens. Due to that limitation, it is possible (although difficult) for an attacker to calculate a future CSRF token value and to use that value to trick a user into executing unwanted actions on an application.<br>**CVE ID : CVE-2021-26296** | d9b%40%3Cannounce.apache.org%3E |  |
| **livy** |  |  |  |  |  |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Feb-21 | 3.5 | Livy server version 0.7.0-incubating (only) is vulnerable to a cross site scripting issue in the session name. A malicious user could use this flaw to access logs and results of other users' sessions and run jobs with their privileges. This issue is fixed in Livy 0.7.1-incubating.<br>**CVE ID : CVE-2021-26544** | http://www.openwall.com/lists/oss-security/2021/02/20/1, https://github.com/apache/incubator-livy/commit/4d8a912699683b973eee76d4e91447d769a0cb0d | A-APA-LIVY-020321/10 |
| **Apereo** |  |  |  |  |  |
| **opencast** |  |  |  |  |  |
| Incorrect Authorization | 18-Feb-21 | 5.5 | Opencast is a free, open-source platform to support the management of educational audio and video content. In Opencast before version 9.2 there is a vulnerability in which publishing an episode with strict access rules will overwrite the currently set series access. This allows for an easy denial of access for all users without superuser | https://github.com/opencast/opencast/commit/b18c6a7f81f08ed14884592a6c14c9ab611ad450, https://github.com/opencast/opencast/security/advisories/GHS | A-APE-OPEN-020321/11 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges, effectively hiding the series. Access to series and series metadata on the search service (shown in media module and player) depends on the events published which are part of the series. Publishing an event will automatically publish a series and update access to it. Removing an event or republishing the event should do the same. Affected versions of Opencast may not update the series access or remove a published series if an event is being removed. On removal of an episode, this may lead to an access control list for series metadata with broader access rules than the merged access rules of all remaining events, or the series metadata still being available although all episodes of that series have been removed. This problem is fixed in Opencast 9.2.<br>**CVE ID : CVE-2021-21318** | A-vpc2-3wcv-qj4w | |
| **appspace** | | | | | |
| **appspace** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Feb-21 | 3.5 | A stored XSS issue exists in Appspace 6.2.4. After a user is authenticated and enters an XSS payload under the groups section of the network tab, it is stored as the group name. Whenever another member visits that group, this payload | N/A | A-APP-APPS-020321/12 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | executes.<br>**CVE ID : CVE-2021-27564** | | |
| **Arubanetworks** | | | | | |
| **clearpass_policy_manager** | | | | | |
| Improper Privilege Management | 23-Feb-21 | 7.2 | A local authenticated escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in ClearPass OnGuard could allow local authenticated users on a Windows platform to elevate their privileges. A successful exploit could allow an attacker to execute arbitrary code with SYSTEM level privileges.<br>**CVE ID : CVE-2021-26677** | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | A-ARU-CLEA-020321/13 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Feb-21 | 9 | A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.<br>**CVE ID : CVE-2021-26679** | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | A-ARU-CLEA-020321/14 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Feb-21 | 9 | A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.<br>**CVE ID : CVE-2021-26680** | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | A-ARU-CLEA-020321/15 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 23-Feb-21 | 4.3 | A remote reflected cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the guest portal interface of ClearPass could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the portal. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the guest portal interface.<br>**CVE ID : CVE-2021-26682** | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | A-ARU-CLEA-020321/16 |
| Improper Neutralizatio | 23-Feb-21 | 9 | A remote authenticated command injection | https://www.arubanetw | A-ARU-CLEA- |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in a Command ('Command Injection') | | | vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.<br>**CVE ID : CVE-2021-26683** | orks.com/assets/alert/ARUBA-PSA-2021-004.txt | 020321/17 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 23-Feb-21 | 9 | A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.<br>**CVE ID : CVE-2021-26684** | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | A-ARU-CLEA-020321/18 |
| Improper Neutralization of Special Elements | 23-Feb-21 | 5.5 | A remote authenticated SQL Injection vulnerabilitiy was discovered in Aruba ClearPass Policy Manager | https://www.arubanetworks.com/assets/alert/AR | A-ARU-CLEA-020321/19 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface API of ClearPass could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database.<br>**CVE ID : CVE-2021-26685** | UBA-PSA-2021-004.txt | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 23-Feb-21 | 5.5 | A remote authenticated SQL Injection vulnerabilitiy was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface API of ClearPass could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database.<br>**CVE ID : CVE-2021-26686** | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | A-ARU-CLEA-020321/20 |
| **Atlassian** | | | | | |
| **jira** | | | | | |
| Improper Neutralization of Special Elements in Output Used | 22-Feb-21 | 9 | An endpoint in Atlassian Jira Server for Slack plugin from version 0.0.3 before version 2.0.15 allows remote attackers to execute arbitrary | https://confluence.atlassian.com/jira/jira-server-for-slack- | A-ATL-JIRA-020321/21 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| by a Downstream Component ('Injection') | | | code via a template injection vulnerability.<br>**CVE ID : CVE-2021-26068** | security-advisory-17th-february-2021-1044091690.html | |
| **Avahi** | | | | | |
| **avahi** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 17-Feb-21 | 4.6 | avahi-daemon-check-dns.sh in the Debian avahi package through 0.8-4 is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. NOTE: this only affects the packaging for Debian GNU/Linux (used indirectly by SUSE), not the upstream Avahi product.<br>**CVE ID : CVE-2021-26720** | N/A | A-AVA-AVAH-020321/22 |
| **baby_care_system_project** | | | | | |
| **baby_care_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Feb-21 | 7.5 | Baby Care System v1.0 is vulnerable to SQL injection via the 'id' parameter on the contentsectionpage.php page.<br>**CVE ID : CVE-2021-25779** | N/A | A-BAB-BABY-020321/23 |
| Unrestricted Upload of | 17-Feb-21 | 6.5 | An arbitrary file upload vulnerability has been | N/A | A-BAB-BABY- |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| File with Dangerous Type | | | identified in posts.php in Baby Care System 1.0. The vulnerability could be exploited by an remote attacker to upload content to the server, including PHP files, which could result in command execution and obtaining a shell.<br>**CVE ID : CVE-2021-25780** | | 020321/24 |
| **Blackcat-cms** | | | | | |
| **blackcat_cms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | The admin panel in BlackCat CMS 1.3.6 allows stored XSS (by an admin) via the Display Name field to backend/preferences/ajax_save.php.<br>**CVE ID : CVE-2021-27237** | https://github.com/BlackCatDevelopment/BlackCatCMS/commits/release-1.4/upload/backend/preferences/ajax_save.php, https://github.com/BlackCatDevelopment/BlackCatCMS/compare/1.3.6...1.4Beta | A-BLA-BLAC-020321/25 |
| **bloodhound_project** | | | | | |
| **bloodhound** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 19-Feb-21 | 9.3 | components/Modals/HelpTexts/GenericAll/GenericAll.jsx in Bloodhound <= 4.0.1 allows remote attackers to execute arbitrary system commands when the victim imports a malicious data file containing JavaScript in the | N/A | A-BLO-BLOO-020321/26 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | objectId parameter.<br>**CVE ID : CVE-2021-3210** | | |
| **boltcms** | | | | | |
| **bolt** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Feb-21 | 5 | Controller/Backend/FileEditController.php and Controller/Backend/FilemanagerController.php in Bolt before 4.1.13 allow Directory Traversal.<br>**CVE ID : CVE-2021-27367** | https://github.com/bolt/core/pull/2371 | A-BOL-BOLT-020321/27 |
| **botan_project** | | | | | |
| **botan** | | | | | |
| Not Available | 22-Feb-21 | 7.5 | In Botan before 2.17.3, constant-time computations are not used for certain decoding and encoding operations (base32, base58, base64, and hex).<br>**CVE ID : CVE-2021-24115** | https://botan.randombit.net/news.html, https://github.com/randombit/botan/compare/2.17.2...2.17.3, https://github.com/randombit/botan/pull/2549 | A-BOT-BOTA-020321/28 |
| **canarymail** | | | | | |
| **canary_mail** | | | | | |
| Improper Certificate Validation | 17-Feb-21 | 5.8 | core/imap/MCIMAPSession.cpp in Canary Mail before 3.22 has Missing SSL Certificate Validation for IMAP in STARTTLS mode.<br>**CVE ID : CVE-2021-26911** | http://www.openwall.com/lists/oss-security/2021/02/17/3, https://github.com/canarymail/mailcore2/commit/ | A-CAN-CANA-020321/29 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 45acb4efbcaa57a20ac5127dc976538671fce018, https://www.openwall.com/lists/oss-security/2021/02/17/3 | |
| **car_rental_portal_project** | | | | | |
| **car_rental_portal** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 17-Feb-21 | 7.5 | PHPGurukul Car Rental Project version 2.0 suffers from a remote shell upload vulnerability in changeimage1.php.<br>**CVE ID : CVE-2021-26809** | N/A | A-CAR-CAR_-020321/30 |
| **Chamilo** | | | | | |
| **chamilo** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-21 | 4.3 | Chamilo 1.11.14 allows XSS via a main/calendar/agenda_list.php?type= URI.<br>**CVE ID : CVE-2021-26746** | https://github.com/chamilo/chamilo-lms/commit/d939402d83bf68af5377b629883d8e5437d843ec, https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-45-2021-01-21-Moderate-impact-moderate- | A-CHA-CHAM-020321/31 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | risk-XSS-vulnerability-in-agenda | |
| **changjia_property_management_system_project** | | | | | |
| **changjia_property_management_system** | | | | | |
| Improper Authentication | 17-Feb-21 | 6.5 | Attackers can access the CGE account management function without privilege for permission elevation and execute arbitrary commands or files after obtaining user permissions.<br>**CVE ID : CVE-2021-22858** | https://www.chtsecurity.com/news/fe1e30ef-4dac-4848-a3c9-a7df12672422 | A-CHA-CHAN-020321/32 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Feb-21 | 5 | The CGE property management system contains SQL Injection vulnerabilities. Remote attackers can inject SQL commands into the parameters in Cookie and obtain data in the database without privilege.<br>**CVE ID : CVE-2021-22856** | https://www.chtsecurity.com/news/fe1e30ef-4dac-4848-a3c9-a7df12672422 | A-CHA-CHAN-020321/33 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Feb-21 | 5 | The CGE page with download function contains a Directory Traversal vulnerability. Attackers can use this loophole to download system files arbitrarily.<br>**CVE ID : CVE-2021-22857** | https://www.chtsecurity.com/news/fe1e30ef-4dac-4848-a3c9-a7df12672422 | A-CHA-CHAN-020321/34 |
| **cira** | | | | | |
| **canadian_shield** | | | | | |
| Improper Certificate Validation | 23-Feb-21 | 4.3 | The CIRA Canadian Shield app before 4.0.13 for iOS lacks SSL Certificate Validation.<br>**CVE ID : CVE-2021-27189** | https://www.info-sec.ca/advisories/CIRA-Canadian- | A-CIR-CANA-020321/35 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | Shield.html | |
| **Cisco** | | | | | |
| **anyconnect_secure_mobility_client** | | | | | |
| Improper Verification of Cryptographic Signature | 17-Feb-21 | 6.9 | A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker needs valid credentials on the Windows system.<br>**CVE ID : CVE-2021-1366** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-hijac-JrcTOQMC | A-CIS-ANYC-020321/36 |
| **webex_meetings_server** | | | | | |
| Exposure of Sensitive Information Through Data Queries | 17-Feb-21 | 2.1 | A vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated, local attacker to gain access to | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | A-CIS-WEBE-020321/37 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sensitive information on an affected system. This vulnerability is due to the unsafe usage of shared memory by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens. Note: To exploit this vulnerability, an attacker must have valid credentials on a Microsoft Windows end-user system and must log in after another user has already authenticated with Webex on the same end-user system.<br>**CVE ID : CVE-2021-1372** | sa-wda-pt-msh-6LWOcZ5 | |
| **identity_services_engine** | | | | | |
| Incorrect Privilege Assignment | 17-Feb-21 | 4 | Multiple vulnerabilities in the Admin portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information. These vulnerabilities are due to improper enforcement of administrator privilege levels for sensitive data. An attacker with read-only administrator | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-exp-8RsuEu8S | A-CIS-IDEN-020321/38 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | access to the Admin portal could exploit these vulnerabilities by browsing to one of the pages that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2021-1412** | | |
| Incorrect Privilege Assignment | 17-Feb-21 | 4 | Multiple vulnerabilities in the Admin portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information. These vulnerabilities are due to improper enforcement of administrator privilege levels for sensitive data. An attacker with read-only administrator access to the Admin portal could exploit these vulnerabilities by browsing to one of the pages that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2021-1416** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-exp-8RsuEu8S | A-CIS-IDEN-020321/39 |
| **webex_meetings** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) | 17-Feb-21 | 4.3 | A vulnerability in the web-based interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected service. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected service. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.<br>**CVE ID : CVE-2021-1351** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-Lz6HbGCt | A-CIS-WEBE-020321/40 |
| Exposure of Sensitive Information Through Data Queries | 17-Feb-21 | 2.1 | A vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. This vulnerability is due to the unsafe usage of shared memory by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wda-pt-msh-6LWOcZ5 | A-CIS-WEBE-020321/41 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens. Note: To exploit this vulnerability, an attacker must have valid credentials on a Microsoft Windows end-user system and must log in after another user has already authenticated with Webex on the same end-user system.<br>**CVE ID : CVE-2021-1372** | | |
| **collaboraoffice** | | | | | |
| **online** | | | | | |
| Improper Privilege Management | 23-Feb-21 | 7.2 | "loolforkit" is a privileged program that is supposed to be run by a special, non-privileged "lool" user. Before doing anything else "loolforkit" checks, if it was invoked by the "lool" user, and refuses to run with privileges, if it's not the case. In the vulnerable version of "loolforkit" this check was wrong, so a normal user could start "loolforkit" and eventually get local root privileges.<br>**CVE ID : CVE-2021-25630** | N/A | A-COL-ONLI-020321/42 |
| **containous** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **traefik** | | | | | |
| Exposure of Resource to Wrong Sphere | 18-Feb-21 | 5 | Traefik before 2.4.5 allows the loading of IFRAME elements from other domains.<br>**CVE ID : CVE-2021-27375** | https://github.com/traefik/traefik/pull/7904, https://github.com/traefik/traefik/releases/tag/v2.4.5 | A-CON-TRAE-020321/43 |
| **custom_global_variables_project** | | | | | |
| **custom_global_variables** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 25-Feb-21 | 3.5 | Stored cross-site scripting (XSS) in form field in robust.systems product Custom Global Variables v 1.0.5 allows a remote attacker to inject arbitrary code via the vars[0][name] field.<br>**CVE ID : CVE-2021-3124** | N/A | A-CUS-CUST-020321/44 |
| **dekart** | | | | | |
| **private_disk** | | | | | |
| NULL Pointer Dereference | 16-Feb-21 | 4.9 | In Dekart Private Disk 2.15, invalid use of the Type3 user buffer for IOCTL codes using METHOD_NEITHER results in arbitrary memory dereferencing.<br>**CVE ID : CVE-2021-27203** | https://www.dekart.com/products/encryption/private_disk | A-DEK-PRIV-020321/45 |
| **Dell** | | | | | |
| **emc_powerprotect_cyber_recovery** | | | | | |
| Exposure of Sensitive Information to an Unauthorize | 19-Feb-21 | 3.6 | Dell EMC PowerProtect Cyber Recovery, version 19.7.0.1, contains an Information Disclosure vulnerability. A locally authenticated high | https://www.dell.com/support/kbdoc/en-us/0001831 | A-DEL-EMC_-020321/46 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| d Actor | | | privileged Cyber Recovery user may potentially exploit this vulnerability leading to the takeover of the notification email account.<br>**CVE ID : CVE-2021-21512** | 69/dsa-2021-038-dell-emc-powerprotect-cyber-recovery-security-update-for-unintended-information-disclosure | |
| **denx** | | | | | |
| **u-boot** | | | | | |
| Not Available | 17-Feb-21 | 6.8 | The boot loader in Das U-Boot before 2021.04-rc2 mishandles a modified FIT.<br>**CVE ID : CVE-2021-27097** | https://github.com/u-boot/u-boot/commit/6f3c2d8aa5e6cbd80b5e869bbbddecb66c329d01, https://github.com/u-boot/u-boot/commit/8a7d4cf9820ea16fabd25a6379351b4dc291204b, https://github.com/u-boot/u-boot/commit/b6f4c757959f8850e1299a77c8e5713da78e8ec0 | A-DEN-U-BO-020321/47 |
| Not Available | 17-Feb-21 | 6.8 | The boot loader in Das U-Boot before 2021.04-rc2 mishandles use of unit | https://github.com/u-boot/u- | A-DEN-U-BO- |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | addresses in a FIT.<br>**CVE ID : CVE-2021-27138** | boot/commit/3f04db891a353f4b127ed57279279f851c6b4917, https://github.com/u-boot/u-boot/commit/79af75f7776fc20b0d7eb6afe1e27c00fdb4b9b4, https://github.com/u-boot/u-boot/commit/b6f4c757959f8850e1299a77c8e5713da78e8ec0 | 020321/48 |
| **Digium** | | | | | |
| **certified_asterisk** | | | | | |
| Not Available | 18-Feb-21 | 5 | Incorrect access controls in res_srtp.c in Sangoma Asterisk 13.38.1, 16.16.0, 17.9.1, and 18.2.0 and Certified Asterisk 16.8-cert5 allow a remote unauthenticated attacker to prematurely terminate secure calls by replaying SRTP packets.<br>**CVE ID : CVE-2021-26712** | https://downloads.asterisk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-003.html, https://issues.asterisk.org/jira/browse/ASTERISK-29260 | A-DIG-CERT-020321/49 |
| Out-of-bounds | 19-Feb-21 | 4 | A stack-based buffer overflow in res_rtp_asterisk.c in | https://downloads.asteri | A-DIG-CERT- |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | Sangoma Asterisk before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6 allows an authenticated WebRTC client to cause an Asterisk crash by sending multiple hold/unhold requests in quick succession. This is caused by a signedness comparison mismatch.<br>**CVE ID : CVE-2021-26713** | sk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-004.html, https://issues.asterisk.org/jira/browse/ASTERISK-29205 | 020321/50 |
| Not Available | 18-Feb-21 | 5 | An issue was discovered in Sangoma Asterisk 16.x before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6. When re-negotiating for T.38, if the initial remote response was delayed just enough, Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a declined T.38 stream, then Asterisk would crash.<br>**CVE ID : CVE-2021-26717** | http://seclists.org/fulldisclosure/2021/Feb/58, https://downloads.asterisk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-002.html, https://issues.asterisk.org/jira/browse/ASTERISK-29203 | A-DIG-CERT-020321/51 |
| Improper Resource Shutdown or Release | 18-Feb-21 | 4.3 | An issue was discovered in res_pjsip_session.c in Digium Asterisk through 13.38.1; 14.x, 15.x, and 16.x through 16.16.0; 17.x through 17.9.1; and 18.x through 18.2.0, and Certified Asterisk through 16.8-cert5. An SDP | http://seclists.org/fulldisclosure/2021/Feb/61, https://downloads.asterisk.org/pub/security/, | A-DIG-CERT-020321/52 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | negotiation vulnerability in PJSIP allows a remote server to potentially crash Asterisk by sending specific SIP responses that cause an SDP negotiation failure.<br>**CVE ID : CVE-2021-26906** | https://downloads.asterisk.org/pub/security/AST-2021-005.html, https://issues.asterisk.org/jira/browse/ASTERISK-29196 | |
| **asterisk** | | | | | |
| Not Available | 18-Feb-21 | 5 | Incorrect access controls in res_srtp.c in Sangoma Asterisk 13.38.1, 16.16.0, 17.9.1, and 18.2.0 and Certified Asterisk 16.8-cert5 allow a remote unauthenticated attacker to prematurely terminate secure calls by replaying SRTP packets.<br>**CVE ID : CVE-2021-26712** | https://downloads.asterisk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-003.html, https://issues.asterisk.org/jira/browse/ASTERISK-29260 | A-DIG-ASTE-020321/53 |
| Out-of-bounds Write | 19-Feb-21 | 4 | A stack-based buffer overflow in res_rtp_asterisk.c in Sangoma Asterisk before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6 allows an authenticated WebRTC client to cause an Asterisk crash by sending multiple hold/unhold requests in quick succession. This is caused by a signedness | https://downloads.asterisk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-004.html, https://issues.asterisk.org/jira/browse | A-DIG-ASTE-020321/54 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | comparison mismatch.<br>**CVE ID : CVE-2021-26713** | /ASTERISK-29205 | |
| Not Available | 18-Feb-21 | 5 | An issue was discovered in Sangoma Asterisk 16.x before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6. When re-negotiating for T.38, if the initial remote response was delayed just enough, Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a declined T.38 stream, then Asterisk would crash.<br>**CVE ID : CVE-2021-26717** | http://seclists.org/fulldisclosure/2021/Feb/58, https://downloads.asterisk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-002.html, https://issues.asterisk.org/jira/browse/ASTERISK-29203 | A-DIG-ASTE-020321/55 |
| Improper Resource Shutdown or Release | 18-Feb-21 | 4.3 | An issue was discovered in res_pjsip_session.c in Digium Asterisk through 13.38.1; 14.x, 15.x, and 16.x through 16.16.0; 17.x through 17.9.1; and 18.x through 18.2.0, and Certified Asterisk through 16.8-cert5. An SDP negotiation vulnerability in PJSIP allows a remote server to potentially crash Asterisk by sending specific SIP responses that cause an SDP negotiation failure.<br>**CVE ID : CVE-2021-26906** | http://seclists.org/fulldisclosure/2021/Feb/61, https://downloads.asterisk.org/pub/security/, https://downloads.asterisk.org/pub/security/AST-2021-005.html, https://issues.asterisk.org/jira/browse/ASTERISK-29196 | A-DIG-ASTE-020321/56 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **docsifyjs** | | | | | |
| **docsify** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-21 | 4.3 | This affects the package docsify before 4.12.0. It is possible to bypass the remediation done by CVE-2020-7680 and execute malicious JavaScript through the following methods 1) When parsing HTML from remote URLs, the HTML code on the main page is sanitized, but this sanitization is not taking place in the sidebar. 2) The isURL external check can be bypassed by inserting more "////" characters<br>**CVE ID : CVE-2021-23342** | https://github.com/docsifyjs/docsify/commit/ff2a66f12752471277fe81a64ad6c4b2c08111fe | A-DOC-DOCS-020321/57 |
| **doctor_appointment_system_project** | | | | | |
| **doctor_appointment_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-21 | 4 | SQL injection in the expertise parameter in search_result.php in Doctor Appointment System v1.0 allows an authenticated patient user to dump the database credentials via a SQL injection attack.<br>**CVE ID : CVE-2021-27124** | N/A | A-DOC-DOCT-020321/58 |
| **Eyesofnetwork** | | | | | |
| **eyesofnetwork** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 22-Feb-21 | 6.5 | The module admin_ITSM in EyesOfNetwork 5.3-10 allows remote authenticated users to upload arbitrary .xml.php files because it relies on "le filtre userside." | https://github.com/EyesOfNetworkCommunity/eonweb/issues/87 | A-EYE-EYES-020321/59 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-27513** | | |
| Improper Restriction of Excessive Authentication Attempts | 22-Feb-21 | 7.5 | EyesOfNetwork 5.3-10 uses an integer of between 8 and 10 digits for the session ID, which might be leveraged for brute-force authentication bypass (such as in CVE-2021-27513 exploitation).<br>**CVE ID : CVE-2021-27514** | https://github.com/EyesOfNetworkCommunity/eonweb/issues/87 | A-EYE-EYES-020321/60 |
| **Fedoraproject** | | | | | |
| **extra_packages_for_enterprise_linux** | | | | | |
| Improper Input Validation | 23-Feb-21 | 5.8 | A flaw was found in mbsync before v1.3.5 and v1.4.1. Validations of the mailbox names returned by IMAP LIST/LSUB do not occur allowing a malicious or compromised server to use specially crafted mailbox names containing '..' path components to access data outside the designated mailbox on the opposite end of the synchronization channel. The highest threat from this vulnerability is to data confidentiality and integrity.<br>**CVE ID : CVE-2021-20247** | N/A | A-FED-EXTR-020321/61 |
| **frendi** | | | | | |
| **frendica** | | | | | |
| Server-Side Request Forgery (SSRF) | 18-Feb-21 | 10 | Friendica 2021.01 allows SSRF via parse_url?binurl= for DNS lookups or HTTP requests to arbitrary domain names.<br>**CVE ID : CVE-2021-27329** | N/A | A-FRE-FREN-020321/62 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **genymobile** | | | | | |
| **genymotion_desktop** | | | | | |
| Cleartext Storage of Sensitive Information | 22-Feb-21 | 5 | ** DISPUTED ** Genymotion Desktop through 3.2.0 leaks the host's clipboard data to the Android application by default. NOTE: the vendor's position is that this is intended behavior that can be changed through the Settings > Device screen.<br>**CVE ID : CVE-2021-27549** | https://docs.genymotion.com/desktop/latest/02_Application.html | A-GEN-GENY-020321/63 |
| **GNU** | | | | | |
| **glibc** | | | | | |
| Double Free | 24-Feb-21 | 4.9 | The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.<br>**CVE ID : CVE-2021-27645** | https://sourceware.org/bugzilla/show_bug.cgi?id=27462 | A-GNU-GLIB-020321/64 |
| **Google** | | | | | |
| **gerrit** | | | | | |
| Uncontrolled Resource Consumption | 17-Feb-21 | 5 | Any git operation is passed through Jetty and a session is created. No expiry is set for the session and Jetty does not automatically dispose of the session. Over multiple git actions, this can lead to a heap memory exhaustion for Gerrit servers. We | https://bugs.chromium.org/p/gerrit/issues/detail?id=13858 | A-GOO-GERR-020321/65 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | recommend upgrading Gerrit to any of the versions listed above.<br>**CVE ID : CVE-2021-22553** | | |
| **chrome** | | | | | |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Stack buffer overflow in Data Transfer in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.<br>**CVE ID : CVE-2021-21149** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1138143 | A-GOO-CHRO-020321/66 |
| Use After Free | 22-Feb-21 | 6.8 | Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.<br>**CVE ID : CVE-2021-21150** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1172192 | A-GOO-CHRO-020321/67 |
| Use After Free | 22-Feb-21 | 6.8 | Use after free in Payments in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.<br>**CVE ID : CVE-2021-21151** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbu | A-GOO-CHRO-020321/68 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | g.com/1165624 | |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Heap buffer overflow in Media in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.<br>**CVE ID : CVE-2021-21152** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1166504 | A-GOO-CHRO-020321/69 |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Stack buffer overflow in GPU Process in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.<br>**CVE ID : CVE-2021-21153** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1155974 | A-GOO-CHRO-020321/70 |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Heap buffer overflow in Tab Strip in Google Chrome prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.<br>**CVE ID : CVE-2021-21154** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1173269 | A-GOO-CHRO-020321/71 |
| Out-of-bounds | 22-Feb-21 | 6.8 | Heap buffer overflow in Tab Strip in Google Chrome on | https://chromereleases.g | A-GOO-CHRO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.<br>**CVE ID : CVE-2021-21155** | oogleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1175500 | 020321/72 |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted script.<br>**CVE ID : CVE-2021-21156** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1177341 | A-GOO-CHRO-020321/73 |
| Use After Free | 22-Feb-21 | 6.8 | Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.<br>**CVE ID : CVE-2021-21157** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1170657 | A-GOO-CHRO-020321/74 |
| **slashify** | | | | | |
| URL Redirection to Untrusted Site ('Open | 19-Feb-21 | 5.8 | The slashify package 1.0.0 for Node.js allows open-redirect attacks, as demonstrated by a localhost:3000///example.co | N/A | A-GOO-SLAS-020321/75 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Redirect') | | | m/ substring.<br>**CVE ID : CVE-2021-3189** | | |
| **hestiacp** | | | | | |
| **control_panel** | | | | | |
| Not Available | 16-Feb-21 | 5.5 | Hestia Control Panel through 1.3.3, in a shared-hosting environment, sometimes allows remote authenticated users to create a subdomain for a different customer's domain name, leading to spoofing of services or email messages.<br>**CVE ID : CVE-2021-27231** | https://www.hestiacp.com/ | A-HES-CONT-020321/76 |
| **hr_portal_project** | | | | | |
| **hr_portal** | | | | | |
| Improper Privilege Management | 17-Feb-21 | 5.5 | The HR Portal of Soar Cloud System fails to manage access control. While obtaining user ID, remote attackers can access sensitive data via a specific data packet, such as userâ€™s login information, further causing the login function not to work.<br>**CVE ID : CVE-2021-22853** | https://www.chtsecurity.com/news/d334641f-2b28-4eab-a5ed-c6ec6740557e | A-HR_-HR_P-020321/77 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 17-Feb-21 | 5 | The HR Portal of Soar Cloud System fails to filter specific parameters. Remote attackers can inject SQL syntax and obtain all data in the database without privilege.<br>**CVE ID : CVE-2021-22854** | https://www.chtsecurity.com/news/d334641f-2b28-4eab-a5ed-c6ec6740557e | A-HR_-HR_P-020321/78 |
| Deserialization of | 17-Feb-21 | 7.5 | The specific function of HR Portal of Soar Cloud System | https://www.chtsecurity | A-HR_-HR_P-020321/79 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Data | | | accepts any type of object to be deserialized. Attackers can send malicious serialized objects to execute arbitrary commands.<br>**CVE ID : CVE-2021-22855** | .com/news/d334641f-2b28-4eab-a5ed-c6ec6740557e | |
| **IBM** | | | | | |
| **websphere_application_server** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883, https://www.ibm.com/support/pages/node/6415959 | A-IBM-WEBS-020321/80 |
| **maximo_for_civil_infrastructure** | | | | | |
| Inclusion of Functionality from Untrusted Control Sphere | 18-Feb-21 | 6.5 | IBM Maximo for Civil Infrastructure 7.6.2 includes executable functionality (such as a library) from a source that is outside of the intended control sphere. IBM X-Force ID: 196619.<br>**CVE ID : CVE-2021-20443** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196619, https://www.ibm.com/support/pages/node/6415883 | A-IBM-MAXI-020321/81 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-21 | 4.3 | IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality | https://exchange.xforce.ibmcloud.com/vulnerabilities/196620, https://www.ibm.com/support/page | A-IBM-MAXI-020321/82 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196620.<br>**CVE ID : CVE-2021-20444** | s/node/6415887 | |
| Insufficiently Protected Credentials | 18-Feb-21 | 4 | IBM Maximo for Civil Infrastructure 7.6.2 could allow a user to obtain sensitive information due to insecure storeage of authentication credentials. IBM X-Force ID: 196621.<br>**CVE ID : CVE-2021-20445** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196621, https://www.ibm.com/support/pages/node/6415891 | A-IBM-MAXI-020321/83 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-21 | 3.5 | IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196622.<br>**CVE ID : CVE-2021-20446** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196622, https://www.ibm.com/support/pages/node/6415893 | A-IBM-MAXI-020321/84 |
| **Irfanview** | | | | | |
| **irfanview** | | | | | |
| Out-of-bounds Write | 17-Feb-21 | 5 | The WPG plugin before 3.1.0.0 for IrfanView 4.57 has a user-mode write access violation starting at WPG+0x0000000000012ec6, which might allow remote attackers to execute arbitrary code. | https://www.irfanview.com/plugins.htm | A-IRF-IRFA-020321/85 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-27224** | | |
| Out-of-bounds Read | 17-Feb-21 | 7.5 | The WPG plugin before 3.1.0.0 for IrfanView 4.57 has a Read Access Violation on Control Flow starting at WPG!ReadWPG_W+0x0000000000000133, which might allow remote attackers to execute arbitrary code.<br>**CVE ID : CVE-2021-27362** | https://www.irfanview.com/plugins.htm | A-IRF-IRFA-020321/86 |
| **wpg** | | | | | |
| Out-of-bounds Write | 17-Feb-21 | 5 | The WPG plugin before 3.1.0.0 for IrfanView 4.57 has a user-mode write access violation starting at WPG+0x0000000000012ec6, which might allow remote attackers to execute arbitrary code.<br>**CVE ID : CVE-2021-27224** | https://www.irfanview.com/plugins.htm | A-IRF-WPG-020321/87 |
| Out-of-bounds Read | 17-Feb-21 | 7.5 | The WPG plugin before 3.1.0.0 for IrfanView 4.57 has a Read Access Violation on Control Flow starting at WPG!ReadWPG_W+0x0000000000000133, which might allow remote attackers to execute arbitrary code.<br>**CVE ID : CVE-2021-27362** | https://www.irfanview.com/plugins.htm | A-IRF-WPG-020321/88 |
| **jasper_project** | | | | | |
| **jasper** | | | | | |
| Out-of-bounds Read | 23-Feb-21 | 5.8 | A flaw was found in jasper before 2.0.25. An out of bounds read issue was found in jp2_decode function whic may lead to disclosure of information or program crash. | https://github.com/jasper-software/jasper/commit/41f214b121b837fa30d9c | A-JAS-JASP-020321/89 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-26926** | a5f2430212110f5cd9b | |
| NULL Pointer Dereference | 23-Feb-21 | 4.3 | A flaw was found in jasper before 2.0.25. A null pointer dereference in jp2_decode in jp2_dec.c may lead to program crash and denial of service.<br>**CVE ID : CVE-2021-26927** | https://github.com/jasper-software/jasper/commit/41f214b121b837fa30d9ca5f2430212110f5cd9b, https://github.com/jasper-software/jasper/issues/265 | A-JAS-JASP-020321/90 |
| **Jenkins** | | | | | |
| **active_choices** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 24-Feb-21 | 3.5 | Jenkins Active Choices Plugin 2.5.2 and earlier does not escape reference parameter values, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.<br>**CVE ID : CVE-2021-21616** | https://www.jenkins.io/security/advisory/2021-02-24/#SECURITY-2192 | A-JEN-ACTI-020321/91 |
| **support_core** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 24-Feb-21 | 5 | Jenkins Support Core Plugin 2.72 and earlier provides the serialized user authentication as part of the "About user (basic authentication details only)" information, which can include the session ID of the user creating the support bundle in some | https://www.jenkins.io/security/advisory/2021-02-24/#SECURITY-2150 | A-JEN-SUPP-020321/92 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | configurations.<br>**CVE ID : CVE-2021-21621** | | |
| **repository_connector** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 24-Feb-21 | 3.5 | Jenkins Repository Connector Plugin 2.0.2 and earlier does not escape parameter names and descriptions for past builds, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.<br>**CVE ID : CVE-2021-21618** | https://www.jenkins.io/security/advisory/2021-02-24/#SECURITY-2183 | A-JEN-REPO-020321/93 |
| **configuration_slicing** | | | | | |
| Cross-Site Request Forgery (CSRF) | 24-Feb-21 | 6.8 | A cross-site request forgery (CSRF) vulnerability in Jenkins Configuration Slicing Plugin 1.51 and earlier allows attackers to apply different slice configurations.<br>**CVE ID : CVE-2021-21617** | https://www.jenkins.io/security/advisory/2021-02-24/#SECURITY-2003 | A-JEN-CONF-020321/94 |
| **claim** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 24-Feb-21 | 3.5 | Jenkins Claim Plugin 2.18.1 and earlier does not escape the user display name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers who are able to control the display names of Jenkins users, either via the security realm, or directly inside Jenkins.<br>**CVE ID : CVE-2021-21619** | https://www.jenkins.io/security/advisory/2021-02-24/#SECURITY-2188%20(1) | A-JEN-CLAI-020321/95 |
| Cross-Site Request Forgery | 24-Feb-21 | 4.3 | A cross-site request forgery (CSRF) vulnerability in Jenkins Claim Plugin 2.18.1 and earlier allows attackers | https://www.jenkins.io/security/advisory/2021- | A-JEN-CLAI-020321/96 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| (CSRF) | | | to change claims.<br>**CVE ID : CVE-2021-21620** | 02-24/#SECURITY-2188%20(2) | |
| **artifact_repository_parameter** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 24-Feb-21 | 3.5 | Jenkins Artifact Repository Parameter Plugin 1.0.0 and earlier does not escape parameter names and descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.<br>**CVE ID : CVE-2021-21622** | https://www.jenkins.io/security/advisory/2021-02-24/#SECURITY-2168 | A-JEN-ARTI-020321/97 |
| **jsdom_project** | | | | | |
| **jsdom** | | | | | |
| Not Available | 16-Feb-21 | 6.8 | JSDom improperly allows the loading of local resources, which allows for local files to be manipulated by a malicious web page when script execution is enabled.<br>**CVE ID : CVE-2021-20066** | N/A | A-JSD-JSDO-020321/98 |
| **keybase** | | | | | |
| **keybase** | | | | | |
| Cleartext Storage of Sensitive Information | 23-Feb-21 | 2.1 | Keybase Desktop Client before 5.6.0 on Windows and macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It fails to effectively clear cached pictures, even after deletion via normal methodology within the | N/A | A-KEY-KEYB-020321/99 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.<br>**CVE ID : CVE-2021-23827** | | |
| **kollectapp** | | | | | |
| **kollect** | | | | | |
| Deserialization of Untrusted Data | 18-Feb-21 | 7.5 | KollectApps before 4.8.16c is affected by insecure Java deserialization, leading to Remote Code Execution via a ysoserial.payloads.Commons Collections parameter.<br>**CVE ID : CVE-2021-27335** | N/A | A-KOL-KOLL-020321/100 |
| **less-openui5_project** | | | | | |
| **less-openui5** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 16-Feb-21 | 6.8 | less-openui5 is an npm package which enables building OpenUI5 themes with Less.js. In less-openui5 before version 0.10., when processing theming resources (i.e. `*.less` files) with less-openui5 that originate from an untrusted source, those resources might contain JavaScript code which will be executed in the context of the build process. While this is a feature of the Less.js library it is an unexpected behavior in the context of OpenUI5 and SAPUI5 development. Especially in the context of UI5 Tooling which relies on less-openui5. An attacker might create a library or | https://github.com/SAP/less-openui5/commit/c0d3a8572974a20ea6cee42da11c614a54f100e8, https://github.com/SAP/less-openui5/security/advisories/GHSA-3crj-w4f5-gwh4 | A-LES-LESS-020321/101 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | theme-library containing a custom control or theme, hiding malicious JavaScript code in one of the .less files. Refer to the referenced GHSA-3crj-w4f5-gwh4 for examples. Starting with Less.js version 3.0.0, the Inline JavaScript feature is disabled by default. less-openui5 however currently uses a fork of Less.js v1.6.3. Note that disabling the Inline JavaScript feature in Less.js versions 1.x, still evaluates code has additional double codes around it. We decided to remove the inline JavaScript evaluation feature completely from the code of our Less.js fork. This fix is available in less-openui5 version 0.10.0.<br>**CVE ID : CVE-2021-21316** | | |
| **libmailcore** | | | | | |
| **mailcore2** | | | | | |
| Improper Certificate Validation | 17-Feb-21 | 5.8 | core/imap/MCIMAPSession.cpp in Canary Mail before 3.22 has Missing SSL Certificate Validation for IMAP in STARTTLS mode.<br>**CVE ID : CVE-2021-26911** | http://www.openwall.com/lists/oss-security/2021/02/17/3, https://github.com/canarymail/mailcore2/commit/45acb4efbcaa57a20ac5127dc976538671fce018, https://ww | A-LIB-MAIL-020321/102 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | w.openwall.com/lists/oss-security/2021/02/17/3 | |
| **lightbend** | | | | | |
| **akka-http** | | | | | |
| Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') | 17-Feb-21 | 6.4 | This affects all versions of package com.typesafe.akka:akka-http-core. It allows multiple Transfer-Encoding headers.<br>**CVE ID : CVE-2021-23339** | N/A | A-LIG-AKKA-020321/103 |
| **lightcms_project** | | | | | |
| **lightcms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 24-Feb-21 | 3.5 | A stored-self XSS exists in LightCMS v1.3.4, allowing an attacker to execute HTML or JavaScript code in a vulnerable Title field to /admin/SensitiveWords.<br>**CVE ID : CVE-2021-3355** | N/A | A-LIG-LIGH-020321/104 |
| **luxion** | | | | | |
| **keyshot_viewer** | | | | | |
| Out-of-bounds Read | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code. | N/A | A-LUX-KEYS-020321/105 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-22643** | | |
| Not Available | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an attack because the .bip documents display a "load" command, which can be pointed to a .dll from a remote network share. As a result, the .dll entry point can be executed without sufficient UI warning.<br>**CVE ID : CVE-2021-22645** | N/A | A-LUX-KEYS-020321/106 |
| Out-of-bounds Write | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to multiple out-of-bounds write issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22647** | N/A | A-LUX-KEYS-020321/107 |
| NULL Pointer Dereference | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 have multiple NULL pointer dereference issues while | N/A | A-LUX-KEYS-020321/108 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22649** |  |  |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 23-Feb-21 | 6.8 | When loading a specially crafted file, Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are, while processing the extraction of temporary files, suffering from a directory traversal vulnerability, which allows an attacker to store arbitrary scripts into automatic startup folders.<br>**CVE ID : CVE-2021-22651** | https://us-cert.cisa.gov/ics/advisories/icsa-21-035-01 | A-LUX-KEYS-020321/109 |
| **keyvr** |  |  |  |  |  |
| Out-of-bounds Read | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22643** | N/A | A-LUX-KEYV-020321/110 |
| Not Available | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to | N/A | A-LUX-KEYV-020321/111 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an attack because the .bip documents display a "load" command, which can be pointed to a .dll from a remote network share. As a result, the .dll entry point can be executed without sufficient UI warning.<br>**CVE ID : CVE-2021-22645** | | |
| Out-of-bounds Write | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to multiple out-of-bounds write issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22647** | N/A | A-LUX-KEYV-020321/112 |
| NULL Pointer Dereference | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 have multiple NULL pointer dereference issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22649** | N/A | A-LUX-KEYV-020321/113 |
| Improper Limitation of | 23-Feb-21 | 6.8 | When loading a specially crafted file, Luxion KeyShot | https://us-cert.cisa.gov/ | A-LUX-KEYV-020321/114 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| a Pathname to a Restricted Directory ('Path Traversal') | | | versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are, while processing the extraction of temporary files, suffering from a directory traversal vulnerability, which allows an attacker to store arbitrary scripts into automatic startup folders.<br>**CVE ID : CVE-2021-22651** | ics/advisories/icsa-21-035-01 | |
| **keyshot** | | | | | |
| Out-of-bounds Read | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22643** | N/A | A-LUX-KEYS-020321/115 |
| Not Available | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an attack because the .bip documents display a “load” command, which can be pointed to a .dll | N/A | A-LUX-KEYS-020321/116 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from a remote network share. As a result, the .dll entry point can be executed without sufficient UI warning.<br>**CVE ID : CVE-2021-22645** | | |
| Out-of-bounds Write | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to multiple out-of-bounds write issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22647** | N/A | A-LUX-KEYS-020321/117 |
| NULL Pointer Dereference | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 have multiple NULL pointer dereference issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22649** | N/A | A-LUX-KEYS-020321/118 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 23-Feb-21 | 6.8 | When loading a specially crafted file, Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 | https://us-cert.cisa.gov/ics/advisories/icsa-21-035-01 | A-LUX-KEYS-020321/119 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | are, while processing the extraction of temporary files, suffering from a directory traversal vulnerability, which allows an attacker to store arbitrary scripts into automatic startup folders.<br>**CVE ID : CVE-2021-22651** | | |
| **keyshot_network_rendering** | | | | | |
| Out-of-bounds Read | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22643** | N/A | A-LUX-KEYS-020321/120 |
| Not Available | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an attack because the .bip documents display a “load” command, which can be pointed to a .dll from a remote network share. As a result, the .dll entry point can be executed without sufficient UI warning.<br>**CVE ID : CVE-2021-22645** | N/A | A-LUX-KEYS-020321/121 |
| Out-of- | 23-Feb-21 | 6.8 | Luxion KeyShot versions | N/A | A-LUX-KEYS- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to multiple out-of-bounds write issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22647** | | 020321/122 |
| NULL Pointer Dereference | 23-Feb-21 | 6.8 | Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 have multiple NULL pointer dereference issues while processing project files, which may allow an attacker to execute arbitrary code.<br>**CVE ID : CVE-2021-22649** | N/A | A-LUX-KEYS-020321/123 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 23-Feb-21 | 6.8 | When loading a specially crafted file, Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are, while processing the extraction of temporary files, suffering from a directory traversal vulnerability, which allows an attacker to store arbitrary scripts into automatic startup folders. | https://us-cert.cisa.gov/ics/advisories/icsa-21-035-01 | A-LUX-KEYS-020321/124 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-22651** | | |
| **mbsync_project** | | | | | |
| **mbsync** | | | | | |
| Improper Input Validation | 23-Feb-21 | 5.8 | A flaw was found in mbsync before v1.3.5 and v1.4.1. Validations of the mailbox names returned by IMAP LIST/LSUB do not occur allowing a malicious or compromised server to use specially crafted mailbox names containing '..' path components to access data outside the designated mailbox on the opposite end of the synchronization channel. The highest threat from this vulnerability is to data confidentiality and integrity.<br>**CVE ID : CVE-2021-20247** | N/A | A-MBS-MBSY-020321/125 |
| **Mcafee** | | | | | |
| **web_gateway** | | | | | |
| Improper Privilege Management | 17-Feb-21 | 9 | Privilege escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.8 allows an authenticated user to gain elevated privileges through the User Interface and execute commands on the appliance via incorrect improper neutralization of user input in the troubleshooting page.<br>**CVE ID : CVE-2021-23885** | https://kc.mcafee.com/corporate/index?page=content&id=SB10349 | A-MCA-WEB_-020321/126 |
| **Microsoft** | | | | | |
| **mono** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Not Available | 25-Feb-21 | 7.5 | .NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26701.<br>**CVE ID : CVE-2021-24112** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24112 | A-MIC-MONO-020321/127 |
| **.net_core** | | | | | |
| Not Available | 25-Feb-21 | 4.3 | .NET Core and Visual Studio Denial of Service Vulnerability<br>**CVE ID : CVE-2021-1721** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721 | A-MIC-.NET-020321/128 |
| Not Available | 25-Feb-21 | 7.5 | .NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26701.<br>**CVE ID : CVE-2021-24112** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24112 | A-MIC-.NET-020321/129 |
| Not Available | 25-Feb-21 | 7.5 | .NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24112.<br>**CVE ID : CVE-2021-26701** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26701 | A-MIC-.NET-020321/130 |
| **visual_studio_2017** | | | | | |
| Not Available | 25-Feb-21 | 4.3 | .NET Core and Visual Studio Denial of Service Vulnerability<br>**CVE ID : CVE-2021-1721** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721 | A-MIC-VISU-020321/131 |
| **visual_studio_2019** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Not Available | 25-Feb-21 | 4.3 | .NET Core and Visual Studio Denial of Service Vulnerability<br>**CVE ID : CVE-2021-1721** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721 | A-MIC-VISU-020321/132 |
| Not Available | 25-Feb-21 | 7.5 | .NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26701.<br>**CVE ID : CVE-2021-24112** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24112 | A-MIC-VISU-020321/133 |
| **.net** | | | | | |
| Not Available | 25-Feb-21 | 4.3 | .NET Core and Visual Studio Denial of Service Vulnerability<br>**CVE ID : CVE-2021-1721** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721 | A-MIC-.NET-020321/134 |
| Not Available | 25-Feb-21 | 7.5 | .NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26701.<br>**CVE ID : CVE-2021-24112** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24112 | A-MIC-.NET-020321/135 |
| Not Available | 25-Feb-21 | 7.5 | .NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24112.<br>**CVE ID : CVE-2021-26701** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26701 | A-MIC-.NET-020321/136 |
| **modernflow** | | | | | |
| Improper Authenticati | 19-Feb-21 | 4 | ModernFlow before 1.3.00.208 does not constrain | N/A | A-MIC-MODE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on | | | web-page access to members of a security group, as demonstrated by the Search Screen and the Profile Screen.<br>**CVE ID : CVE-2021-3339** | | 020321/137 |
| **monicahq** | | | | | |
| **monica** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Feb-21 | 3.5 | The Contact page in Monica 2.19.1 allows stored XSS via the First Name field.<br>**CVE ID : CVE-2021-27368** | N/A | A-MON-MONI-020321/138 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Feb-21 | 3.5 | The Contact page in Monica 2.19.1 allows stored XSS via the Middle Name field.<br>**CVE ID : CVE-2021-27369** | N/A | A-MON-MONI-020321/139 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Feb-21 | 3.5 | The Contact page in Monica 2.19.1 allows stored XSS via the Last Name field.<br>**CVE ID : CVE-2021-27370** | N/A | A-MON-MONI-020321/140 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 22-Feb-21 | 3.5 | The Contact page in Monica 2.19.1 allows stored XSS via the Description field.<br>**CVE ID : CVE-2021-27371** | N/A | A-MON-MONI-020321/141 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 22-Feb-21 | 3.5 | The Contact page in Monica 2.19.1 allows stored XSS via the Nickname field.<br>**CVE ID : CVE-2021-27559** | N/A | A-MON-MONI-020321/142 |
| **Mumble** | | | | | |
| **mumble** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 16-Feb-21 | 6.8 | Mumble before 1.3.4 allows remote code execution if a victim navigates to a crafted URL on a server list and clicks on the Open Webpage text.<br>**CVE ID : CVE-2021-27229** | https://github.com/mumble-voip/mumble/commit/e59ee87abe249f345908c7d568f6879d16bfd648, https://github.com/mumble-voip/mumble/compare/1.3.3...1.3.4, https://github.com/mumble-voip/mumble/pull/4733 | A-MUM-MUMB-020321/143 |
| **Mutare** | | | | | |
| **voice** | | | | | |
| Cleartext Storage of Sensitive Information | 16-Feb-21 | 4 | An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. On the admin portal of the web application, password information for external systems is visible in | https://www.mutare.com/security-adv-mutare-2021-004-mutare- | A-MUT-VOIC-020321/144 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | cleartext. The Settings.asp page is affected by this issue.<br>**CVE ID : CVE-2021-27233** | voice/ | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Feb-21 | 7.5 | An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. The web application suffers from SQL injection on Adminlog.asp, Archivemsgs.asp, Deletelog.asp, Eventlog.asp, and Evmlog.asp.<br>**CVE ID : CVE-2021-27234** | https://www.mutare.com/security-adv-mutare-2021-002-mutare-voice/ | A-MUT-VOIC-020321/145 |
| Not Available | 16-Feb-21 | 4 | An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. On the admin portal of the web application, there is a functionality at diagzip.asp that allows anyone to export tables of a database.<br>**CVE ID : CVE-2021-27235** | https://www.mutare.com/security-adv-mutare-2021-003-mutare-voice/ | A-MUT-VOIC-020321/146 |
| Improper Control of Generation of Code ('Code Injection') | 16-Feb-21 | 7.5 | An issue was discovered in Mutare Voice (EVM) 3.x before 3.3.8. getfile.asp allows Unauthenticated Local File Inclusion, which can be leveraged to achieve Remote Code Execution.<br>**CVE ID : CVE-2021-27236** | https://www.mutare.com/security-adv-mutare-2021-001-mutare-voice/ | A-MUT-VOIC-020321/147 |
| **Mybb** | | | | | |
| **mybb** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 22-Feb-21 | 3.5 | MyBB before 1.8.25 allows stored XSS via nested [email] tags with MyCode (aka BBCode).<br>**CVE ID : CVE-2021-27279** | https://github.com/mybb/mybb/commit/cb781b49116bf5c4d8deca3e17498122b70167 | A-MYB-MYBB-020321/148 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | | 7a, https://github.com/mybb/mybb/security/advisories/GHSA-6483-hcpp-p75w, https://mybb.com/versions/1.8.25/ | |
| **nb-connect_project** | | | | | |
| **nb-connect** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 18-Feb-21 | 7.5 | An issue was discovered in the nb-connect crate before 1.0.3 for Rust. It may have invalid memory access for certain versions of the standard library because it relies on a direct cast of std::net::SocketAddrV4 and std::net::SocketAddrV6 data structures.<br>**CVE ID : CVE-2021-27376** | N/A | A-NB--NB-C-020321/149 |
| **nozominetworks** | | | | | |
| **central_management_control** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Feb-21 | 9 | OS Command Injection vulnerability when changing date settings or hostname using web GUI of Nozomi Networks Guardian and CMC allows authenticated administrators to perform remote code execution. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 | https://security.nozominetworks.com/NN-2021:1-01 | A-NOZ-CENT-020321/150 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and prior versions.<br>**CVE ID : CVE-2021-26724** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 22-Feb-21 | 4 | Path Traversal vulnerability when changing timezone using web GUI of Nozomi Networks Guardian, CMC allows an authenticated administrator to read-protected system files. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.<br>**CVE ID : CVE-2021-26725** | https://security.nozominetworks.com/NN-2021:2-01 | A-NOZ-CENT-020321/151 |
| **guardian** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Feb-21 | 9 | OS Command Injection vulnerability when changing date settings or hostname using web GUI of Nozomi Networks Guardian and CMC allows authenticated administrators to perform remote code execution. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.<br>**CVE ID : CVE-2021-26724** | https://security.nozominetworks.com/NN-2021:1-01 | A-NOZ-GUAR-020321/152 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path | 22-Feb-21 | 4 | Path Traversal vulnerability when changing timezone using web GUI of Nozomi Networks Guardian, CMC allows an authenticated administrator to read-protected system files. This | https://security.nozominetworks.com/NN-2021:2-01 | A-NOZ-GUAR-020321/153 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Traversal') | | | issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.<br>**CVE ID : CVE-2021-26725** | | |
| **openenergymonitor** | | | | | |
| **emoncms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Feb-21 | 4.3 | Modules/input/Views/schedule.php in Emoncms through 10.2.7 allows XSS via the node parameter.<br>**CVE ID : CVE-2021-26716** | N/A | A-OPE-EMON-020321/154 |
| **Opennms** | | | | | |
| **horizon** | | | | | |
| Incorrect Authorization | 17-Feb-21 | 6.5 | OpenNMS Meridian 2016, 2017, 2018 before 2018.1.25, 2019 before 2019.1.16, and 2020 before 2020.1.5, Horizon 1.2 through 27.0.4, and Newts <1.5.3 has Incorrect Access Control, which allows local and remote code execution using JEXL expressions.<br>**CVE ID : CVE-2021-3396** | https://www.opennms.com, https://www.opennms.com/en/blog/2021-02-16-cve-2021-3396-full-security-disclosure/ | A-OPE-HORI-020321/155 |
| **meridian** | | | | | |
| Incorrect Authorization | 17-Feb-21 | 6.5 | OpenNMS Meridian 2016, 2017, 2018 before 2018.1.25, 2019 before 2019.1.16, and 2020 before 2020.1.5, Horizon 1.2 through 27.0.4, and Newts <1.5.3 has Incorrect Access Control, | https://www.opennms.com, https://www.opennms.com/en/blog/2021-02-16- | A-OPE-MERI-020321/156 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which allows local and remote code execution using JEXL expressions.<br>**CVE ID : CVE-2021-3396** | cve-2021-3396-full-security-disclosure/ | |
| **newts** | | | | | |
| Incorrect Authorization | 17-Feb-21 | 6.5 | OpenNMS Meridian 2016, 2017, 2018 before 2018.1.25, 2019 before 2019.1.16, and 2020 before 2020.1.5, Horizon 1.2 through 27.0.4, and Newts <1.5.3 has Incorrect Access Control, which allows local and remote code execution using JEXL expressions.<br>**CVE ID : CVE-2021-3396** | https://www.opennms.com, https://www.opennms.com/en/blog/2021-02-16-cve-2021-3396-full-security-disclosure/ | A-OPE-NEWT-020321/157 |
| **Openssl** | | | | | |
| **openssl** | | | | | |
| Inadequate Encryption Strength | 16-Feb-21 | 5 | OpenSSL 1.0.2 supports SSLv2. If a client attempts to negotiate SSLv2 with a server that is configured to support both SSLv2 and more recent SSL and TLS versions then a check is made for a version rollback attack when unpadding an RSA signature. Clients that support SSL or TLS versions greater than SSLv2 are supposed to use a special form of padding. A server that supports greater than SSLv2 is supposed to reject connection attempts from a client where this special form of padding is present, because this indicates that a version rollback has occurred (i.e. | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=30919ab80a478f2d81f2e9acdcca3fa4740cd547, https://security.netapp.com/advisory/ntap-20210219-0009/, https://www.openssl.org/news/secadv/20210216.txt | A-OPE-OPEN-020321/158 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | both client and server support greater than SSLv2, and yet this is the version that is being requested). The implementation of this padding check inverted the logic so that the connection attempt is accepted if the padding is present, and rejected if it is absent. This means that such as server will accept a connection if a version rollback attack has occurred. Further the server will erroneously reject a connection if a normal SSLv2 connection attempt is made. Only OpenSSL 1.0.2 servers from version 1.0.2s to 1.0.2x are affected by this issue. In order to be vulnerable a 1.0.2 server must: 1) have configured SSLv2 support at compile time (this is off by default), 2) have configured SSLv2 support at runtime (this is off by default), 3) have configured SSLv2 ciphersuites (these are not in the default ciphersuite list) OpenSSL 1.1.1 does not have SSLv2 support and therefore is not vulnerable to this issue. The underlying error is in the implementation of the RSA_padding_check_SSLv23() function. This also affects the RSA_SSLV23_PADDING padding mode used by various other functions. Although 1.1.1 does not |  |  |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | support SSLv2 the RSA_padding_check_SSLv23() function still exists, as does the RSA_SSLV23_PADDING padding mode. Applications that directly call that function or use that padding mode will encounter this issue. However since there is no support for the SSLv2 protocol in 1.1.1 this is considered a bug and not a security issue in that version. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.0.2y (Affected 1.0.2s-1.0.2x).<br>**CVE ID : CVE-2021-23839** | | |
| Integer Overflow or Wraparound | 16-Feb-21 | 5 | Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=6a51b9e1d0cf0bf8515f7201b68fb0a3482b3dc1, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=9b1129239f3ebb1d1c98ce | A-OPE-OPEN-020321/159 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).<br>**CVE ID : CVE-2021-23840** | 9ed41d5c9476c47cb2, https://www.openssl.org/news/secadv/20210216.txt |  |
| Integer Overflow or Wraparound | 16-Feb-21 | 5 | The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=122a19ab48091c657f7cb1fb3af9fc07bd557bbf, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8252ee4d90f3f2004d3d0aeeed003ad49c9a7807, https://www.openssl.org/news/secadv/2021021 | A-OPE-OPEN-020321/160 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).<br>**CVE ID : CVE-2021-23841** | 6.txt |  |
| **pelco** |  |  |  |  |  |
| **digital_sentry_server** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 6.8 | The RTSPLive555.dll ActiveX control in Pelco Digital Sentry Server 7.18.72.11464 has a SetCameraConnectionParameter stack-based buffer overflow. This can be exploited by a remote attacker to potentially execute arbitrary attacker-supplied code. The victim would have to visit a malicious webpage using Internet Explorer where the exploit could be triggered.<br>**CVE ID : CVE-2021-27232** | https://support.pelco.com/s/article/What-is-the-Digital-Sentry-software-release-revision-history | A-PEL-DIGI-020321/161 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Pimcore** | | | | | |
| **pimcore** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 5.5 | This affects the package pimcore/pimcore before 6.8.8. A Local FIle Inclusion vulnerability exists in the downloadCsvAction function of the CustomReportController class (bundles/AdminBundle/Controller/Reports/CustomReportController.php). An authenticated user can reach this function with a GET request at the following endpoint: /admin/reports/custom-report/download-csv?exportFile=&91;filename]. Since exportFile variable is not sanitized, an attacker can exploit a local file inclusion vulnerability.<br>**CVE ID : CVE-2021-23340** | https://github.com/pimcore/pimcore/commit/1786bdd4962ee51544fad537352c2b4223309442, https://snyk.io/vuln/SNYK-PHP-PIMCOREPIMCORE-1070132 | A-PIM-PIMC-020321/162 |
| **polarisoffice** | | | | | |
| **polaris_office** | | | | | |
| Divide By Zero | 23-Feb-21 | 4.3 | Polaris Office v9.102.66 is affected by a divide-by-zero error in PolarisOffice.exe and EngineDLL.dll that may cause a local denial of service. To exploit the vulnerability, someone must open a crafted PDF file.<br>**CVE ID : CVE-2021-27550** | N/A | A-POL-POLA-020321/163 |
| **Postgresql** | | | | | |
| **postgresql** | | | | | |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Authorization | 23-Feb-21 | 4 | A flaw was found in PostgreSQL in versions before 13.2, before 12.6, before 11.11, before 10.16, before 9.6.21 and before 9.5.25. This flaw allows a user with SELECT privilege on one column to craft a special query that returns all columns of the table. The highest threat from this vulnerability is to confidentiality.<br>**CVE ID : CVE-2021-20229** | N/A | A-POS-POST-020321/164 |
| **pressbooks** | | | | | |
| **pressbooks** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-21 | 3.5 | PressBooks 5.17.3 contains a cross-site scripting (XSS). Stored XSS can be submitted via the Book Info's Long Description Body, and all actions to open or preview the books page will result in the triggering the stored XSS.<br>**CVE ID : CVE-2021-3271** | N/A | A-PRE-PRES-020321/165 |
| **prismjs** | | | | | |
| **prism** | | | | | |
| Not Available | 18-Feb-21 | 5 | The package prismjs before 1.23.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the prism-asciidoc, prism-rest, prism-tap and prism-eiffel components.<br>**CVE ID : CVE-2021-23341** | https://github.com/PrismJS/prism/commit/c2f6a64426f44497a675cb32dccb079b3eff1609, https://github.com/PrismJS/prism/iss | A-PRI-PRIS-020321/166 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | ues/2583, https://github.com/PrismJS/prism/pull/2584, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1076583 | |
| **rand_core_project** | | | | | |
| **rand_core** | | | | | |
| Use of Insufficiently Random Values | 18-Feb-21 | 7.5 | An issue was discovered in the rand_core crate before 0.6.2 for Rust. Because read_u32_into and read_u64_into mishandle certain buffer-length checks, a random number generator may be seeded with too little data.<br>**CVE ID : CVE-2021-27378** | N/A | A-RAN-RAND-020321/167 |
| **Redhat** | | | | | |
| **software_collections** | | | | | |
| Incorrect Authorization | 23-Feb-21 | 4 | A flaw was found in PostgreSQL in versions before 13.2, before 12.6, before 11.11, before 10.16, before 9.6.21 and before 9.5.25. This flaw allows a user with SELECT privilege on one column to craft a special query that returns all columns of the table. The highest threat from this vulnerability is to confidentiality.<br>**CVE ID : CVE-2021-20229** | N/A | A-RED-SOFT-020321/168 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **3scale_api_management** | | | | | |
| Improper Input Validation | 23-Feb-21 | 6.8 | A flaw was found in Red Hat 3scale API Management Platform 2. The 3scale backend does not perform preventive handling on user-requested date ranges in certain queries allowing a malicious authenticated user to submit a request with a sufficiently large date range to eventually yield an internal server error resulting in denial of service. The highest threat from this vulnerability is to system availability.<br>**CVE ID : CVE-2021-20252** | https://bugzilla.redhat.com/show_bug.cgi?id=1928302 | A-RED-3SCA-020321/169 |
| **openshift_container_platform** | | | | | |
| Files or Directories Accessible to External Parties | 23-Feb-21 | 6.5 | A privilege escalation flaw was found in openshift4/ose-docker-builder. The build container runs with high privileges using a chrooted environment instead of runc. If an attacker can gain access to this build container, they can potentially utilize the raw devices of the underlying node, such as the network and storage devices, to at least escalate their privileges to that of the cluster admin. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.<br>**CVE ID : CVE-2021-20182** | https://bugzilla.redhat.com/show_bug.cgi?id=1915110 | A-RED-OPEN-020321/170 |
| Improper Input | 23-Feb-21 | 4.6 | There is a vulnerability in the linux kernel versions higher | https://bugzilla.redhat.co | A-RED-OPEN- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | than 5.2 (if kernel compiled with config params CONFIG_BPF_SYSCALL=y , CONFIG_BPF=y , CONFIG_CGROUPS=y , CONFIG_CGROUP_BPF=y , CONFIG_HARDENED_USERCOPY not set, and BPF hook to getsockopt is registered). As result of BPF execution, the local user can trigger bug in __cgroup_bpf_run_filter_getsockopt() function that can lead to heap overflow (because of non-hardened usercopy). The impact of attack could be deny of service or possibly privileges escalation.<br>**CVE ID : CVE-2021-20194** | m/show_bug.cgi?id=1912683 | 020321/171 |
| **satellite** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 23-Feb-21 | 4.6 | A flaw was found in Red Hat Satellite. The BMC interface exposes the password through the API to an authenticated local attacker with view_hosts permission. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.<br>**CVE ID : CVE-2021-20256** | https://bugzilla.redhat.com/show_bug.cgi?id=1930926 | A-RED-SATE-020321/172 |
| **openshift_installer** | | | | | |
| Missing Authentication for Critical Function | 23-Feb-21 | 6.8 | A flaw was found in the OpenShift Installer before version v0.9.0-master.0.20210125200451-95101da940b0. During installation of OpenShift Container Platform 4 clusters, | https://bugzilla.redhat.com/show_bug.cgi?id=1920764 | A-RED-OPEN-020321/173 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bootstrap nodes are provisioned with anonymous authentication enabled on kubelet port 10250. A remote attacker able to reach this port during installation can make unauthenticated `/exec` requests to execute arbitrary commands within running containers. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.<br>**CVE ID : CVE-2021-20198** | | |
| **scrapbox-parser_project** | | | | | |
| **scrapbox-parser** | | | | | |
| Uncontrolled Resource Consumption | 19-Feb-21 | 5 | A ReDoS (regular expression denial of service) flaw was found in the @progfay/scrapbox-parser package before 6.0.3 for Node.js.<br>**CVE ID : CVE-2021-27405** | https://github.com/progfay/scrapbox-parser/pull/519, https://github.com/progfay/scrapbox-parser/pull/539, https://github.com/progfay/scrapbox-parser/pull/540 | A-SCR-SCRA-020321/174 |
| **shinobi** | | | | | |
| **shinobi_pro** | | | | | |
| Use of Hard-coded Credentials | 22-Feb-21 | 7.5 | An issue was discovered in Shinobi through ocean version 1. lib/auth.js has Incorrect Access Control. Valid API Keys are held in an | https://gitlab.com/Shinobi-Systems/Shinobi/- | A-SHI-SHIN-020321/175 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | internal JS Object. Therefore an attacker can use JS Proto Method names (such as constructor or hasOwnProperty) to convince the System that the supplied API Key exists in the underlying JS object, and consequently achieve complete access to User/Admin/Super API functions, as demonstrated by a /super/constructor/accounts /list URI.<br>**CVE ID : CVE-2021-27228** | /merge_requests/286, https://gitlab.com/Shinobi-Systems/Shinobi/-/tags | |
| **Smarty** | | | | | |
| **smarty** | | | | | |
| Not Available | 22-Feb-21 | 5 | Smarty before 3.1.39 allows a Sandbox Escape because $smarty.template_object can be accessed in sandbox mode.<br>**CVE ID : CVE-2021-26119** | N/A | A-SMA-SMAR-020321/176 |
| Improper Control of Generation of Code ('Code Injection') | 22-Feb-21 | 7.5 | Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.<br>**CVE ID : CVE-2021-26120** | N/A | A-SMA-SMAR-020321/177 |
| **snowsoftware** | | | | | |
| **snow_inventory** | | | | | |
| Improper Privilege Management | 23-Feb-21 | 6.8 | Snow Inventory Agent through 6.7.0 on Windows uses CPUID to report on processor types and versions that may be deployed and in use across an IT environment. A privilege- | https://community.snowsoftware.com/s/feed/0D56900009cfHLDCA2 | A-SNO-SNOW-020321/178 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation vulnerability exists if CPUID is enabled, and thus it should be disabled via configuration settings.<br>**CVE ID : CVE-2021-27579** | | |
| **soliton** | | | | | |
| **filezen** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 17-Feb-21 | 9 | FileZen (V3.0.0 to V4.2.7 and V5.0.0 to V5.0.2) allows a remote attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.<br>**CVE ID : CVE-2021-20655** | https://www.soliton.co.jp/support/2021/004334.html | A-SOL-FILE-020321/179 |
| **Stunnel** | | | | | |
| **stunnel** | | | | | |
| Improper Certificate Validation | 23-Feb-21 | 5 | A flaw was found in stunnel before 5.57, where it improperly validates client certificates when it is configured to use both redirect and verifyChain options. This flaw allows an attacker with a certificate signed by a Certificate Authority, which is not the one accepted by the stunnel server, to access the tunneled service instead of being redirected to the address specified in the redirect option. The highest threat from this vulnerability is to confidentiality.<br>**CVE ID : CVE-2021-20230** | https://github.com/mtrojnar/stunnel/commit/ebad9ddc4efb2635f37174c9d800d06206f1edf9 | A-STU-STUN-020321/180 |
| **systeminformation** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **systeminformation** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 16-Feb-21 | 4.6 | The System Information Library for Node.JS (npm package "systeminformation") is an open source collection of functions to retrieve detailed hardware, system and OS information. In systeminformation before version 5.3.1 there is a command injection vulnerability. Problem was fixed in version 5.3.1. As a workaround instead of upgrading, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() ... do only allow strings, reject any arrays. String sanitation works as expected.<br>**CVE ID : CVE-2021-21315** | https://github.com/sebhildebrandt/systeminformation/commit/07daa05fb06f24f96297abaa30c2ace8bfd8b525, https://github.com/sebhildebrandt/systeminformation/security/advisories/GHSA-2m8v-572m-ff2v | A-SYS-SYST-020321/181 |
| **Telegram** | | | | | |
| **telegram** | | | | | |
| Insufficient Session Expiration | 19-Feb-21 | 5 | The Terminate Session feature in the Telegram application through 7.2.1 for Android, and through 2.4.7 for Windows and UNIX, fails to invalidate a recently active session.<br>**CVE ID : CVE-2021-27351** | N/A | A-TEL-TELE-020321/182 |
| **testes-codigo** | | | | | |
| **testes_de_codigo** | | | | | |
| Incorrect | 16-Feb-21 | 7.5 | Mobile application "Testes de | N/A | A-TES-TEST- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Authorization | | | Codigo" 11.4 and prior allows an attacker to gain access to the administrative interface and premium features by tampering the boolean value of parameters "isAdmin" and "isPremium" located on device storage.<br>**CVE ID : CVE-2021-25648** | | 020321/183 |
| **uap-core_project** | | | | | |
| **uap-core** | | | | | |
| Uncontrolled Resource Consumption | 16-Feb-21 | 5 | uap-core in an open-source npm package which contains the core of BrowserScope's original user agent string parser. In uap-core before version 0.11.0, some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This is fixed in version 0.11.0. Downstream packages such as uap-python, uap-ruby etc which depend upon uap-core follow different version schemes.<br>**CVE ID : CVE-2021-21317** | https://github.com/ua-parser/uap-core/commit/dc9925d458214cfe87b93e35346980612f6ae96c, https://github.com/ua-parser/uap-core/security/advisories/GHSA-p4pj-mg4r-x6v4 | A-UAP-UAP--020321/184 |
| **ui** | | | | | |
| **unifi_protect_controller** | | | | | |
| Uncontrolled Resource Consumption | 23-Feb-21 | 5 | UniFi Protect before v1.17.1 allows an attacker to use spoofed cameras to perform a denial-of-service attack that | https://community.ui.com/releases/Security- | A-UI-UNIF-020321/185 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may cause the UniFi Protect controller to crash.<br>**CVE ID : CVE-2021-22882** | advisory-bulletin-017-017/071141e5-bc2e-4b71-81f3-5e499316fcee | |
| **urijs_project** | | | | | |
| **urijs** | | | | | |
| Not Available | 22-Feb-21 | 5 | URI.js (aka urijs) before 1.19.6 mishandles certain uses of backslash such as http:\/ and interprets the URI as a relative path.<br>**CVE ID : CVE-2021-27516** | https://github.com/medialize/URI.js/commit/a1ad8bcbc39a4d136d7e252e76e957f3ece70839 | A-URI-URIJ-020321/186 |
| **url-parse_project** | | | | | |
| **url-parse** | | | | | |
| Not Available | 22-Feb-21 | 5 | url-parse before 1.5.0 mishandles certain uses of backslash such as http:\/ and interprets the URI as a relative path.<br>**CVE ID : CVE-2021-27515** | https://github.com/unshiftio/url-parse/commit/d1e7e8822f26e8a49794b757123b51386325b2b0, https://github.com/unshiftio/url-parse/compare/1.4.7...1.5.0, https://github.com/unshiftio/url-parse/pull/197 | A-URL-URL--020321/187 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **vertigis** | | | | | |
| **weboffice** | | | | | |
| Not Available | 17-Feb-21 | 5 | VertiGIS WebOffice 10.7 SP1 before patch20210202 and 10.8 SP1 before patch20210207 allows attackers to achieve "Zugriff auf Inhalte der WebOffice Applikation."<br>**CVE ID : CVE-2021-27374** | https://resources.weboffice.vertigis.com/WebOffice107/Patches/Readme_Patch_de.html#patch20210202, https://resources.weboffice.vertigis.com/WebOffice108/Patches/Readme_Patch_de.html#patch20210207 | A-VER-WEBO-020321/188 |
| **webware** | | | | | |
| **webdesktop** | | | | | |
| Server-Side Request Forgery (SSRF) | 19-Feb-21 | 4 | SSRF in the document conversion component of Webware Webdesktop 5.1.15 allows an attacker to read all files from the server.<br>**CVE ID : CVE-2021-3204** | N/A | A-WEB-WEBD-020321/189 |
| **Wireshark** | | | | | |
| **wireshark** | | | | | |
| Missing Release of Memory after Effective Lifetime | 17-Feb-21 | 5 | Memory leak in USB HID dissector in Wireshark 3.4.0 to 3.4.2 allows denial of service via packet injection or crafted capture file<br>**CVE ID : CVE-2021-22173** | https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22173.json, https://ww | A-WIR-WIRE-020321/190 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | w.wireshark.org/security/wnpa-sec-2021-01.html | |
| Uncontrolled Resource Consumption | 17-Feb-21 | 5 | Crash in USB HID dissector in Wireshark 3.4.0 to 3.4.2 allows denial of service via packet injection or crafted capture file<br>**CVE ID : CVE-2021-22174** | https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22174.json, https://www.wireshark.org/security/wnpa-sec-2021-02.html | A-WIR-WIRE-020321/191 |
| **yithemes** | | | | | |
| **woocommerce_gift_cards** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 22-Feb-21 | 10 | An arbitrary file upload vulnerability in the YITH WooCommerce Gift Cards Premium plugin before 3.3.1 for WordPress allows remote attackers to achieve remote code execution on the operating system in the security context of the web server. In order to exploit this vulnerability, an attacker must be able to place a valid Gift Card product into the shopping cart. An uploaded file is placed at a predetermined path on the web server with a user-specified filename and extension. This occurs because the ywgc-upload- | https://yithemes.com/themes/plugins/yith-woocommerce-gift-cards/ | A-YIT-WOOC-020321/192 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | picture parameter can have a .php value even though the intention was to only allow uploads of Gift Card images.<br>**CVE ID : CVE-2021-3120** | | |
| **yottadb** | | | | | |
| **yottadb** | | | | | |
| Use After Free | 18-Feb-21 | 7.5 | An issue was discovered in the yottadb crate before 1.2.0 for Rust. For some memory-allocation patterns, ydb_subscript_next_st and ydb_subscript_prev_st have a use-after-free.<br>**CVE ID : CVE-2021-27377** | N/A | A-YOT-YOTT-020321/193 |
| **Zohocorp** | | | | | |
| **manageengine_adselfservice_plus** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-21 | 4.3 | A Server-side request forgery (SSRF) vulnerability in the ProductConfig servlet in Zoho ManageEngine ADSelfService Plus through 6013 allows a remote unauthenticated attacker to perform blind HTTP requests or perform a Cross-site scripting (XSS) attack against the administrative interface via an HTTP request, a different vulnerability than CVE-2019-3905.<br>**CVE ID : CVE-2021-27214** | https://www.manageengine.com/products/self-service-password/release-notes.html | A-ZOH-MANA-020321/194 |
| **Operating System** | | | | | |
| **Apple** | | | | | |
| **mac_os** | | | | | |
| Cleartext Storage of | 23-Feb-21 | 2.1 | Keybase Desktop Client before 5.6.0 on Windows and | N/A | O-APP-MAC_- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Sensitive Information | | | macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It fails to effectively clear cached pictures, even after deletion via normal methodology within the client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.<br>**CVE ID : CVE-2021-23827** | | 020321/195 |
| **Asus** | | | | | |
| **askey_rtf8115vw_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-21 | 4.3 | Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow cgi-bin/te_acceso_router.cgi curWebPage XSS.<br>**CVE ID : CVE-2021-27403** | N/A | O-ASU-ASKE-020321/196 |
| URL Redirection to Untrusted Site ('Open Redirect') | 19-Feb-21 | 5.8 | Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow injection of a Host HTTP header.<br>**CVE ID : CVE-2021-27404** | N/A | O-ASU-ASKE-020321/197 |
| **Cisco** | | | | | |
| **staros** | | | | | |
| Uncontrolled Resource Consumption | 17-Feb-21 | 5 | A vulnerability in the SSH service of the Cisco StarOS operating system could allow an unauthenticated, remote | https://tools.cisco.com/security/center/content/Cis | O-CIS-STAR-020321/198 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error that may occur under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to prevent the targeted service from receiving any traffic, which would lead to a DoS condition on the affected device.<br>**CVE ID : CVE-2021-1378** | coSecurityAdvisory/cisco-sa-StarOS-DoS-RLLvGFJj | |
| **Debian** | | | | | |
| **debian_linux** | | | | | |
| Integer Overflow or Wraparound | 16-Feb-21 | 5 | Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=6a51b9e1d0cf0bf8515f7201b68fb0a3482b3dc1, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=9b1129239f3ebb1d1c98ce9ed41d5c9476c47cb2, https://www.openssl.or | O-DEB-DEBI-020321/199 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).<br>**CVE ID : CVE-2021-23840** | g/news/secadv/20210216.txt | |
| Integer Overflow or Wraparound | 16-Feb-21 | 5 | The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=122a19ab48091c657f7cb1fb3af9fc07bd557bbf, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8252ee4d90f3f2004d3d0aeeed003ad49c9a7807, https://www.openssl.org/news/secadv/20210216.txt | O-DEB-DEBI-020321/200 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).<br>**CVE ID : CVE-2021-23841** | | |
| Improper Link Resolution Before File Access ('Link Following') | 17-Feb-21 | 4.6 | avahi-daemon-check-dns.sh in the Debian avahi package through 0.8-4 is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. NOTE: this only affects the packaging for Debian GNU/Linux (used indirectly by SUSE), not the upstream Avahi product.<br>**CVE ID : CVE-2021-26720** | N/A | O-DEB-DEBI-020321/201 |
| Improper Link Resolution Before File Access ('Link Following') | 16-Feb-21 | 6.8 | Mumble before 1.3.4 allows remote code execution if a victim navigates to a crafted URL on a server list and clicks on the Open Webpage text. | https://github.com/mumble-voip/mumble/commit/e59ee87abe24 | O-DEB-DEBI-020321/202 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-27229** | 9f345908c7d568f6879d16bfd648, https://github.com/mumble-voip/mumble/compare/1.3.3...1.3.4, https://github.com/mumble-voip/mumble/pull/4733 | |
| **Fedoraproject** | | | | | |
| **fedora** | | | | | |
| Improper Input Validation | 23-Feb-21 | 5.8 | A flaw was found in mbsync before v1.3.5 and v1.4.1. Validations of the mailbox names returned by IMAP LIST/LSUB do not occur allowing a malicious or compromised server to use specially crafted mailbox names containing '..' path components to access data outside the designated mailbox on the opposite end of the synchronization channel. The highest threat from this vulnerability is to data confidentiality and integrity.<br>**CVE ID : CVE-2021-20247** | N/A | O-FED-FEDO-020321/203 |
| Not Available | 17-Feb-21 | 2.1 | An issue was discovered in Xen 4.9 through 4.14.x. On Arm, a guest is allowed to control whether memory accesses are bypassing the | http://xenbits.xen.org/xsa/advisory-364.html | O-FED-FEDO-020321/204 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | cache. This means that Xen needs to ensure that all writes (such as the ones during scrubbing) have reached the memory before handing over the page to a guest. Unfortunately, the operation to clean the cache is happening before checking if the page was scrubbed. Therefore there is no guarantee when all the writes will reach the memory.<br>**CVE ID : CVE-2021-26933** | | |
| **hilscher** | | | | | |
| **profinet_io_device_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-HIL-PROF-020321/205 |
| **ethernet\/ip_adapter_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery. | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpa | O-HIL-ETHE-020321/206 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-20987** | ge.action?pageId=108969480 | |
| **HP** | | | | | |
| **hp-ux** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883, https://www.ibm.com/support/pages/node/6415959 | O-HP-HP-U-020321/207 |
| **IBM** | | | | | |
| **AIX** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883, https://www.ibm.com/support/pages/node/6415959 | O-IBM-AIX-020321/208 |
| **i** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883, https://www.ibm.com/support/page | O-IBM-I-020321/209 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Traversal') | | | arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | s/node/6415959 | |
| **z\/os** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883, https://www.ibm.com/support/pages/node/6415959 | O-IBM-Z\/O-020321/210 |
| **Intel** | | | | | |
| **compute_stick_stk1a32sc_firmware** | | | | | |
| Not Available | 17-Feb-21 | 4.6 | Insecure inherited permissions for the Intel(R) SOC driver package for STK1A32SC before version 604 may allow an authenticated user to potentially enable escalation of privilege via local access.<br>**CVE ID : CVE-2021-0109** | https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00471.html | O-INT-COMP-020321/211 |
| **kaco-newenergy** | | | | | |
| **xp100u_firmware** | | | | | |
| Insufficiently Protected Credentials | 23-Feb-21 | 5 | KACO New Energy XP100U Up to XP-JAVA 2.0 is affected by incorrect access control. Credentials will always be returned in plain-text from the local server during the KACO XP100U authentication process, regardless of whatever passwords have | N/A | O-KAC-XP10-020321/212 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | been provided, which leads to an information disclosure vulnerability.<br>**CVE ID : CVE-2021-3252** | | |
| **keybase** | | | | | |
| **keybase** | | | | | |
| Cleartext Storage of Sensitive Information | 23-Feb-21 | 2.1 | Keybase Desktop Client before 5.6.0 on Windows and macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It fails to effectively clear cached pictures, even after deletion via normal methodology within the client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.<br>**CVE ID : CVE-2021-23827** | N/A | O-KEY-KEYB-020321/213 |
| **Linux** | | | | | |
| **linux_kernel** | | | | | |
| Improper Input Validation | 23-Feb-21 | 4.6 | There is a vulnerability in the linux kernel versions higher than 5.2 (if kernel compiled with config params CONFIG_BPF_SYSCALL=y , CONFIG_BPF=y , CONFIG_CGROUPS=y , CONFIG_CGROUP_BPF=y , CONFIG_HARDENED_USERCOPY not set, and BPF hook to getsockopt is registered). As result of BPF execution, the | https://bugzilla.redhat.com/show_bug.cgi?id=1912683 | O-LIN-LINU-020321/214 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | local user can trigger bug in __cgroup_bpf_run_filter_getsockopt() function that can lead to heap overflow (because of non-hardened usercopy). The impact of attack could be deny of service or possibly privileges escalation.<br>**CVE ID : CVE-2021-20194** | | |
| Use After Free | 23-Feb-21 | 6.1 | A use-after-free flaw was found in the io_uring in Linux kernel, where a local attacker with a user privilege could cause a denial of service problem on the system The issue results from the lack of validating the existence of an object prior to performing operations on the object by not incrementing the file reference counter while in use. The highest threat from this vulnerability is to data integrity, confidentiality and system availability.<br>**CVE ID : CVE-2021-20226** | N/A | O-LIN-LINU-020321/215 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883, https://www.ibm.com/support/pages/node/6415959 | O-LIN-LINU-020321/216 |
| Inclusion of Functionality | 18-Feb-21 | 6.5 | IBM Maximo for Civil Infrastructure 7.6.2 includes | https://exchange.xforce.i | O-LIN-LINU-020321/217 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| from Untrusted Control Sphere | | | executable functionality (such as a library) from a source that is outside of the intended control sphere. IBM X-Force ID: 196619.<br>**CVE ID : CVE-2021-20443** | bmcloud.com/vulnerabilities/196619, https://www.ibm.com/support/pages/node/6415883 | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-21 | 4.3 | IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196620.<br>**CVE ID : CVE-2021-20444** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196620, https://www.ibm.com/support/pages/node/6415887 | O-LIN-LINU-020321/218 |
| Insufficiently Protected Credentials | 18-Feb-21 | 4 | IBM Maximo for Civil Infrastructure 7.6.2 could allow a user to obtain sensitive information due to insecure storeage of authentication credentials. IBM X-Force ID: 196621.<br>**CVE ID : CVE-2021-20445** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196621, https://www.ibm.com/support/pages/node/6415891 | O-LIN-LINU-020321/219 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-21 | 3.5 | IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to | https://exchange.xforce.ibmcloud.com/vulnerabilities/196622, https://www.ibm.com/support/pages/node/6415 | O-LIN-LINU-020321/220 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | credentials disclosure within a trusted session. IBM X-Force ID: 196622.<br>**CVE ID : CVE-2021-20446** | 893 | |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Stack buffer overflow in Data Transfer in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.<br>**CVE ID : CVE-2021-21149** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1138143 | O-LIN-LINU-020321/221 |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Heap buffer overflow in Media in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.<br>**CVE ID : CVE-2021-21152** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1166504 | O-LIN-LINU-020321/222 |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Stack buffer overflow in GPU Process in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.<br>**CVE ID : CVE-2021-21153** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/11559 | O-LIN-LINU-020321/223 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 74 | |
| Use After Free | 22-Feb-21 | 6.8 | Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.<br>**CVE ID : CVE-2021-21157** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html,<br>https://crbug.com/1170657 | O-LIN-LINU-020321/224 |
| Not Available | 17-Feb-21 | 4.6 | An issue was discovered in the Linux kernel 3.11 through 5.10.16, as used by Xen. To service requests to the PV backend, the driver maps grant references provided by the frontend. In this process, errors may be encountered. In one case, an error encountered earlier might be discarded by later processing, resulting in the caller assuming successful mapping, and hence subsequent operations trying to access space that wasn't mapped. In another case, internal state would be insufficiently updated, preventing safe recovery from the error. This affects drivers/block/xen-blkback/blkback.c.<br>**CVE ID : CVE-2021-26930** | http://xenbits.xen.org/xsa/advisory-365.html | O-LIN-LINU-020321/225 |
| Allocation of Resources Without | 17-Feb-21 | 1.9 | An issue was discovered in the Linux kernel 2.6.39 through 5.10.16, as used in | http://xenbits.xen.org/xsa/advisory- | O-LIN-LINU-020321/226 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Limits or Throttling | | | Xen. Block, net, and SCSI backends consider certain errors a plain bug, deliberately causing a kernel crash. For errors potentially being at least under the influence of guests (such as out of memory conditions), it isn't correct to assume a plain bug. Memory allocations potentially causing such crashes occur only when Linux is running in PV mode, though. This affects drivers/block/xen-blkback/blkback.c and drivers/xen/xen-scsiback.c.<br>**CVE ID : CVE-2021-26931** | 362.html | |
| Not Available | 17-Feb-21 | 1.9 | An issue was discovered in the Linux kernel 3.2 through 5.10.16, as used by Xen. Grant mapping operations often occur in batch hypercalls, where a number of operations are done in a single hypercall, the success or failure of each one is reported to the backend driver, and the backend driver then loops over the results, performing follow-up actions based on the success or failure of each operation. Unfortunately, when running in PV mode, the Linux backend drivers mishandle this: Some errors are ignored, effectively implying their success from the success of related batch elements. In | http://xenbits.xen.org/xsa/advisory-361.html | O-LIN-LINU-020321/227 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | other cases, errors resulting from one batch element lead to further batch elements not being inspected, and hence successful ones to not be possible to properly unmap upon error recovery. Only systems with Linux backends running in PV mode are vulnerable. Linux backends run in HVM / PVH modes are not vulnerable. This affects arch/*/xen/p2m.c and drivers/xen/gntdev.c.<br>**CVE ID : CVE-2021-26932** | | |
| Not Available | 17-Feb-21 | 4.6 | An issue was discovered in the Linux kernel 4.18 through 5.10.16, as used by Xen. The backend allocation (aka be-alloc) mode of the drm_xen_front drivers was not meant to be a supported configuration, but this wasn't stated accordingly in its support status entry.<br>**CVE ID : CVE-2021-26934** | http://xenbits.xen.org/xsa/advisory-363.html | O-LIN-LINU-020321/228 |
| **Microsoft** | | | | | |
| **windows** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883,<br>https://www.ibm.com/support/pages/node/6415959 | O-MIC-WIND-020321/229 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Inclusion of Functionality from Untrusted Control Sphere | 18-Feb-21 | 6.5 | IBM Maximo for Civil Infrastructure 7.6.2 includes executable functionality (such as a library) from a source that is outside of the intended control sphere. IBM X-Force ID: 196619.<br>**CVE ID : CVE-2021-20443** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196619, https://www.ibm.com/support/pages/node/6415883 | O-MIC-WIND-020321/230 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-21 | 4.3 | IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196620.<br>**CVE ID : CVE-2021-20444** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196620, https://www.ibm.com/support/pages/node/6415887 | O-MIC-WIND-020321/231 |
| Insufficiently Protected Credentials | 18-Feb-21 | 4 | IBM Maximo for Civil Infrastructure 7.6.2 could allow a user to obtain sensitive information due to insecure storeage of authentication credentials. IBM X-Force ID: 196621.<br>**CVE ID : CVE-2021-20445** | https://exchange.xforce.ibmcloud.com/vulnerabilities/196621, https://www.ibm.com/support/pages/node/6415891 | O-MIC-WIND-020321/232 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 18-Feb-21 | 3.5 | IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the | https://exchange.xforce.ibmcloud.com/vulnerabilities/196622, https://www.ibm.com/s | O-MIC-WIND-020321/233 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196622.<br>**CVE ID : CVE-2021-20446** | upport/pages/node/6415893 | |
| Out-of-bounds Write | 25-Feb-21 | 6.8 | Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2021-21065** | https://helpx.adobe.com/security/products/bridge/apsb21-07.html | O-MIC-WIND-020321/234 |
| Out-of-bounds Write | 25-Feb-21 | 6.8 | Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2021-21066** | https://helpx.adobe.com/security/products/bridge/apsb21-07.html | O-MIC-WIND-020321/235 |
| Use After Free | 22-Feb-21 | 6.8 | Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, | O-MIC-WIND-020321/236 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-21150** | https://crbug.com/1172192 | |
| Out-of-bounds Write | 22-Feb-21 | 6.8 | Heap buffer overflow in Tab Strip in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.<br>**CVE ID : CVE-2021-21155** | https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html, https://crbug.com/1175500 | O-MIC-WIND-020321/237 |
| Cleartext Storage of Sensitive Information | 23-Feb-21 | 2.1 | Keybase Desktop Client before 5.6.0 on Windows and macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It fails to effectively clear cached pictures, even after deletion via normal methodology within the client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.<br>**CVE ID : CVE-2021-23827** | N/A | O-MIC-WIND-020321/238 |
| Improper Privilege Management | 23-Feb-21 | 7.2 | A local authenticated escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in ClearPass | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt | O-MIC-WIND-020321/239 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | OnGuard could allow local authenticated users on a Windows platform to elevate their privileges. A successful exploit could allow an attacker to execute arbitrary code with SYSTEM level privileges.<br>**CVE ID : CVE-2021-26677** | | |
| **powershell_core** | | | | | |
| Not Available | 25-Feb-21 | 4.3 | .NET Core and Visual Studio Denial of Service Vulnerability<br>**CVE ID : CVE-2021-1721** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721 | O-MIC-POWE-020321/240 |
| **NEC** | | | | | |
| **csdj-b_firmware** | | | | | |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | N/A | O-NEC-CSDJ-020321/241 |
| **csdj-h_firmware** | | | | | |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass | N/A | O-NEC-CSDJ-020321/242 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** |  |  |
| **csdj-d_firmware** |  |  |  |  |  |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | N/A | O-NEC-CSDJ-020321/243 |
| **csdj-a_firmware** |  |  |  |  |  |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | N/A | O-NEC-CSDJ-020321/244 |
| **netis-systems** |  |  |  |  |  |
| **wf2411_firmware** |  |  |  |  |  |
| Improper Neutralization of Special Elements | 18-Feb-21 | 10 | Netis WF2780 2.3.40404 and WF2411 1.1.29629 devices allow Shell Metacharacter Injection into the ping | http://www.netis-systems.com.tw/ | O-NET-WF24-020321/245 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | command, leading to remote code execution.<br>**CVE ID : CVE-2021-26747** | | |
| **wf2780_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-21 | 10 | Netis WF2780 2.3.40404 and WF2411 1.1.29629 devices allow Shell Metacharacter Injection into the ping command, leading to remote code execution.<br>**CVE ID : CVE-2021-26747** | http://www.netis-systems.com.tw/ | O-NET-WF27-020321/246 |
| **netshieldcorp** | | | | | |
| **nano_25_firmware** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 22-Feb-21 | 9 | On Netshield NANO 25 10.2.18 devices, /usr/local/webmin/System/manual_ping.cgi allows OS command injection (after authentication by the attacker) because the system C library function is used unsafely.<br>**CVE ID : CVE-2021-3149** | https://www.netshieldcorp.com/netshield-appliances/ | O-NET-NANO-020321/247 |
| **Oracle** | | | | | |
| **solaris** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-21 | 7.8 | IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. | https://exchange.xforce.ibmcloud.com/vulnerabilities/194883,<br>https://www.ibm.com/support/pages/node/6415 | O-ORA-SOLA-020321/248 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IBM X-Force ID: 194883.<br>**CVE ID : CVE-2021-20354** | 959 | |
| **pepperl-fuchs** | | | | | |
| **pgv100-f200a-b17-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PGV1-020321/249 |
| **pgv150i-f200a-b17-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PGV1-020321/250 |
| **pgv100-f200-b17-v1d-7477_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to | https://cert.vde.com/en-us/advisories/vde-2021- | O-PEP-PGV1-020321/251 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | 006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device |  |
| **pxv100-f200-b17-v1d_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PXV1-020321/252 |
| **pxv100-f200-b17-v1d-3636_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET | O-PEP-PXV1-020321/253 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | +IO+Device | |
| **pcv80-f200-b17-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PCV8-020321/254 |
| **pcv100-f200-b17-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PCV1-020321/255 |
| **pcv50-f200-b17-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/d | O-PEP-PCV5-020321/256 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | isplay/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pcv100-f200-b17-v1d-6011-6997_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PCV1-020321/257 |
| **pcv100-f200-b17-v1d-6011_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PCV1-020321/258 |
| **pcv100-f200-b17-v1d-6011-8203_firmware** | | | | | |
| Out-of- | 16-Feb-21 | 5 | A Denial of Service | https://cert. | O-PEP-PCV1- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | 020321/259 |
| **pxv100a-f200-b28-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PXV1-020321/260 |
| **pxv100a-f200-b28-v1d-6011_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vu | O-PEP-PXV1-020321/261 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | lnerability+in+PROFINET+IO+Device | |
| **pgv100a-f200-b28-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PGV1-020321/262 |
| **pgv100a-f200a-b28-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PGV1-020321/263 |
| **pgv100aq-f200a-b28-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to | https://cert.vde.com/en-us/advisories/vde-2021-006, | O-PEP-PGV1-020321/264 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pgv100aq-f200-b28-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PGV1-020321/265 |
| **pxv100aq-f200-b28-v1d_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PXV1-020321/266 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **pxv100aq-f200-b28-v1d-6011_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PXV1-020321/267 |
| **ohv-f230-b17_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-OHV--020321/268 |
| **oit500-f113b17-cb_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/ | O-PEP-OIT5-020321/269 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | communication.<br>**CVE ID : CVE-2021-20986** | 2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pha_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-PHA_-020321/270 |
| **wcs_firmware** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | O-PEP-WCS_-020321/271 |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in | https://cert.vde.com/en-us/advisorie | O-PEP-WCS_-020321/272 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | s/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 |  |
| **pxv100-f200-b25-v1d_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | O-PEP-PXV1-020321/273 |
| **pxv100i-f200-b25-v1d_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | O-PEP-PXV1-020321/274 |
| **pcv100-f200-b25-v1d-6011-6720_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hi | O-PEP-PCV1-020321/275 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | lscher.com/pages/viewpage.action?pageId=108969480 |  |
| **pcv50-f200-b25-v1d_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | O-PEP-PCV5-020321/276 |
| **pcv80-f200-b25-v1d_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | O-PEP-PCV8-020321/277 |
| **pcv100-f200-b25-v1d-6011_firmware** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery. | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pa | O-PEP-PCV1-020321/278 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-20987** | geId=108969480 | |
| **racom** | | | | | |
| **m\!dge_firmware** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 16-Feb-21 | 5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to view sensitive syslog events without authentication.<br>**CVE ID : CVE-2021-20067** | N/A | O-RAC-M\!D-020321/279 |
| **m\!dge_cellular_router_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the error handling functionality of web pages.<br>**CVE ID : CVE-2021-20068** | N/A | O-RAC-M\!D-020321/280 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the regionalSettings.php dialogs.<br>**CVE ID : CVE-2021-20069** | N/A | O-RAC-M\!D-020321/281 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the virtualization.php dialogs.<br>**CVE ID : CVE-2021-20070** | N/A | O-RAC-M\!D-020321/282 |
| Improper Neutralization of Input | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to | N/A | O-RAC-M\!D-020321/283 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | conduct cross-site scriptings attacks via the sms.php dialogs.<br>**CVE ID : CVE-2021-20071** | | |
| Improper Privilege Management | 16-Feb-21 | 8.7 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to arbitrarily access and delete files via an authenticated directory traveral.<br>**CVE ID : CVE-2021-20072** | N/A | O-RAC-M\!D-020321/284 |
| Cross-Site Request Forgery (CSRF) | 16-Feb-21 | 6.8 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows for cross-site request forgeries.<br>**CVE ID : CVE-2021-20073** | N/A | O-RAC-M\!D-020321/285 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 16-Feb-21 | 9 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows users to escape the provided command line interface and execute arbitrary OS commands.<br>**CVE ID : CVE-2021-20074** | N/A | O-RAC-M\!D-020321/286 |
| Improper Privilege Management | 16-Feb-21 | 7.2 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows for privilege escalation via configd.<br>**CVE ID : CVE-2021-20075** | N/A | O-RAC-M\!D-020321/287 |
| **Redhat** | | | | | |
| **enterprise_linux** | | | | | |
| Improper Input Validation | 23-Feb-21 | 4.6 | There is a vulnerability in the linux kernel versions higher than 5.2 (if kernel compiled with config params CONFIG_BPF_SYSCALL=y , | https://bugzilla.redhat.com/show_bug.cgi?id=1912683 | O-RED-ENTE-020321/288 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CONFIG_BPF=y , CONFIG_CGROUPS=y , CONFIG_CGROUP_BPF=y , CONFIG_HARDENED_USERCOPY not set, and BPF hook to getsockopt is registered). As result of BPF execution, the local user can trigger bug in __cgroup_bpf_run_filter_getsockopt() function that can lead to heap overflow (because of non-hardened usercopy). The impact of attack could be deny of service or possibly privileges escalation.<br>**CVE ID : CVE-2021-20194** | | |
| Incorrect Authorization | 23-Feb-21 | 4 | A flaw was found in PostgreSQL in versions before 13.2, before 12.6, before 11.11, before 10.16, before 9.6.21 and before 9.5.25. This flaw allows a user with SELECT privilege on one column to craft a special query that returns all columns of the table. The highest threat from this vulnerability is to confidentiality.<br>**CVE ID : CVE-2021-20229** | N/A | O-RED-ENTE-020321/289 |
| **linux** | | | | | |
| Cleartext Storage of Sensitive Information | 23-Feb-21 | 2.1 | Keybase Desktop Client before 5.6.0 on Windows and macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It | N/A | O-RED-LINU-020321/290 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | fails to effectively clear cached pictures, even after deletion via normal methodology within the client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.<br>**CVE ID : CVE-2021-23827** | | |
| **se** | | | | | |
| **powerlogic_ion7400_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/291 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/292 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | user and the device.<br>**CVE ID : CVE-2021-22702** | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/293 |
| **powerlogic_ion7650_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/294 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/295 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** |  |  |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/296 |
| **powerlogic_ion8600_firmware** |  |  |  |  |  |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/297 |
| Cleartext Transmissio | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive | https://www.se.com/w | O-SE-POWE-020321/298 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Sensitive Information | | | information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | w/en/download/document/SEVD-2021-040-01/ | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/299 |
| **powerlogic_ion8650_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/300 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/301 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/302 |
| **powerlogic_ion8800_firmware** | | | | | |
| Cross-Site Request Forgery | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic | https://www.se.com/ww/en/downl | O-SE-POWE-020321/303 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| (CSRF) | | | ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | oad/document/SEVD-2021-040-01/ | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/304 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device. | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/305 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-22703** | | |
| **powerlogic_ion9000_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/306 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/307 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/308 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | | |
| **powerlogic_pm8000_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/309 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/310 |
| Cleartext Transmissio | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive | https://www.se.com/w | O-SE-POWE-020321/311 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Sensitive Information | | | information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | w/en/download/document/SEVD-2021-040-01/ | |
| **powerlogic_ion8300_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/312 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/313 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/314 |
| **powerlogic_ion8400_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/315 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, | https://www.se.com/ww/en/download/document/SEVD-2021-040- | O-SE-POWE-020321/316 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | 01/ | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/317 |
| **powerlogic_ion8500_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/318 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/319 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/320 |
| **powerlogic_ion7700_firmware** | | | | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/321 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | | |
| **powerlogic_ion7300_firmware** | | | | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | O-SE-POWE-020321/322 |
| **XEN** | | | | | |
| **xen** | | | | | |
| Not Available | 17-Feb-21 | 2.1 | An issue was discovered in Xen 4.9 through 4.14.x. On Arm, a guest is allowed to control whether memory accesses are bypassing the cache. This means that Xen needs to ensure that all writes (such as the ones during scrubbing) have reached the memory before handing over the page to a | http://xenbits.xen.org/xsa/advisory-364.html | O-XEN-XEN-020321/323 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | guest. Unfortunately, the operation to clean the cache is happening before checking if the page was scrubbed. Therefore there is no guarantee when all the writes will reach the memory.<br>**CVE ID : CVE-2021-26933** | | |
| Improper Privilege Management | 18-Feb-21 | 5.9 | An issue was discovered in Xen through 4.11.x, allowing x86 Intel HVM guest OS users to achieve unintended read/write DMA access, and possibly cause a denial of service (host OS crash) or gain privileges. This occurs because a backport missed a flush, and thus IOMMU updates were not always correct. NOTE: this issue exists because of an incomplete fix for CVE-2020-15565.<br>**CVE ID : CVE-2021-27379** | http://xenbits.xen.org/xsa/advisory-366.html,<br>https://xenbits.xen.org/xsa/advisory-366.html | O-XEN-XEN-020321/324 |
| **yeastar** | | | | | |
| **neogate_tg400_firmware** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 19-Feb-21 | 4 | Yeastar NeoGate TG400 91.3.0.3 devices are affected by Directory Traversal. An authenticated user can decrypt firmware and can read sensitive information, such as a password or decryption key.<br>**CVE ID : CVE-2021-27328** | http://yeastar.com | O-YEA-NEOG-020321/325 |
| **Hardware** | | | | | |
| **Asus** | | | | | |
| **askey_rtf8115vw** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-21 | 4.3 | Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow cgi-bin/te_acceso_router.cgi curWebPage XSS.<br>**CVE ID : CVE-2021-27403** | N/A | H-ASU-ASKE-020321/326 |
| URL Redirection to Untrusted Site ('Open Redirect') | 19-Feb-21 | 5.8 | Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow injection of a Host HTTP header.<br>**CVE ID : CVE-2021-27404** | N/A | H-ASU-ASKE-020321/327 |
| **hilscher** | | | | | |
| **profinet_io_device** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-HIL-PROF-020321/328 |
| **ethernet\/ip_adapter** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpa | H-HIL-ETHE-020321/329 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | 🟥 | crash without recovery.<br>**CVE ID : CVE-2021-20987** | ge.action?pageId=108969480 | |
| **Intel** | | | | | |
| **compute_stick_stk1a32sc** | | | | | |
| Not Available | 17-Feb-21 | 4.6 | Insecure inherited permissions for the Intel(R) SOC driver package for STK1A32SC before version 604 may allow an authenticated user to potentially enable escalation of privilege via local access.<br>**CVE ID : CVE-2021-0109** | https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00471.html | H-INT-COMP-020321/330 |
| **kaco-newenergy** | | | | | |
| **xp100u** | | | | | |
| Insufficiently Protected Credentials | 23-Feb-21 | 5 | KACO New Energy XP100U Up to XP-JAVA 2.0 is affected by incorrect access control. Credentials will always be returned in plain-text from the local server during the KACO XP100U authentication process, regardless of whatever passwords have been provided, which leads to an information disclosure vulnerability.<br>**CVE ID : CVE-2021-3252** | N/A | H-KAC-XP10-020321/331 |
| **NEC** | | | | | |
| **csdj-b** | | | | | |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass | N/A | H-NEC-CSDJ-020321/332 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | | |
| **csdj-h** | | | | | |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | N/A | H-NEC-CSDJ-020321/333 |
| **csdj-d** | | | | | |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | N/A | H-NEC-CSDJ-020321/334 |
| **csdj-a** | | | | | |
| Incorrect Default Permissions | 17-Feb-21 | 5 | Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows | N/A | H-NEC-CSDJ-020321/335 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.<br>**CVE ID : CVE-2021-20653** | | |
| **netis-systems** | | | | | |
| **wf2780** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-21 | 10 | Netis WF2780 2.3.40404 and WF2411 1.1.29629 devices allow Shell Metacharacter Injection into the ping command, leading to remote code execution.<br>**CVE ID : CVE-2021-26747** | http://www.netis-systems.com.tw/ | H-NET-WF27-020321/336 |
| **wf2411** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-21 | 10 | Netis WF2780 2.3.40404 and WF2411 1.1.29629 devices allow Shell Metacharacter Injection into the ping command, leading to remote code execution.<br>**CVE ID : CVE-2021-26747** | http://www.netis-systems.com.tw/ | H-NET-WF24-020321/337 |
| **netshieldcorp** | | | | | |
| **nano_25** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command | 22-Feb-21 | 9 | On Netshield NANO 25 10.2.18 devices, /usr/local/webmin/System/manual_ping.cgi allows OS command injection (after authentication by the attacker) because the system C library function is used | https://www.netshieldcorp.com/netshield-appliances/ | H-NET-NANO-020321/338 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | 🟥 | unsafely.<br>**CVE ID : CVE-2021-3149** | | |
| **pepperl-fuchs** | | | | | |
| **pgv100-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PGV1-020321/339 |
| **pgv150i-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PGV1-020321/340 |
| **pgv100-f200-b17-v1d-7477** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to | https://cert.vde.com/en-us/advisories/vde-2021- | H-PEP-PGV1-020321/341 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | 006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pxv100-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PXV1-020321/342 |
| **pxv100-f200-b17-v1d-3636** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET | H-PEP-PXV1-020321/343 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | +IO+Device | |
| **pcv80-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PCV8-020321/344 |
| **pcv100-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PCV1-020321/345 |
| **pcv50-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/d | H-PEP-PCV5-020321/346 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | isplay/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pcv100-f200-b17-v1d-6011-6997** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PCV1-020321/347 |
| **pcv100-f200-b17-v1d-6011** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PCV1-020321/348 |
| **pcv100-f200-b17-v1d-6011-8203** | | | | | |
| Out-of- | 16-Feb-21 | 5 | A Denial of Service | https://cert. | H-PEP-PCV1- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | 020321/349 |
| **pxv100a-f200-b28-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PXV1-020321/350 |
| **pxv100a-f200-b28-v1d-6011** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vu | H-PEP-PXV1-020321/351 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | lnerability+in+PROFINET+IO+Device | |
| **pgv100a-f200-b28-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PGV1-020321/352 |
| **pgv100a-f200a-b28-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PGV1-020321/353 |
| **pgv100aq-f200a-b28-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to | https://cert.vde.com/en-us/advisories/vde-2021-006, | H-PEP-PGV1-020321/354 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device |  |
| **pgv100aq-f200-b28-v1d** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PGV1-020321/355 |
| **pxv100aq-f200-b28-v1d** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PXV1-020321/356 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **pxv100aq-f200-b28-v1d-6011** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PXV1-020321/357 |
| **ohv-f230-b17** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-OHV--020321/358 |
| **oit500-f113b17-cb** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/ | H-PEP-OIT5-020321/359 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | communication.<br>**CVE ID : CVE-2021-20986** | 2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pha150-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA1-020321/360 |
| **pha150-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA1-020321/361 |
| **pha200-f200-b17-v1d** | | | | | |
| Out-of-bounds | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in | https://cert.vde.com/en- | H-PEP-PHA2- |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | 020321/362 |
| **pha200-f200a-b17-t-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA2-020321/363 |
| **pha200-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+i | H-PEP-PHA2-020321/364 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | n+PROFINET +IO+Device | |
| **pha300-f200-b17-t-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA3-020321/365 |
| **pha300-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA3-020321/366 |
| **pha300-f200a-b17-t-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hi | H-PEP-PHA3-020321/367 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | lscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pha300-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA3-020321/368 |
| **pha400-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA4-020321/369 |
| **pha400-f200a-b17-t-v1d** | | | | | |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA4-020321/370 |
| **pha400-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA4-020321/371 |
| **pha500-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication. | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+o | H-PEP-PHA5-020321/372 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-20986** | f+Service+vulnerability+in+PROFINET+IO+Device | |
| **pha500-f200a-b17-t-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA5-020321/373 |
| **pha500-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA5-020321/374 |
| **pha600-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to | https://cert.vde.com/en-us/advisories/vde-2021- | H-PEP-PHA6-020321/375 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | 006,<br>https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **pha600-f200a-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006,<br>https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA6-020321/376 |
| **pha700-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006,<br>https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET | H-PEP-PHA7-020321/377 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | +IO+Device | |
| **pha800-f200-b17-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-PHA8-020321/378 |
| **wcs3b-ls610** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-WCS3-020321/379 |
| **wcs3b-ls610-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/d | H-PEP-WCS3-020321/380 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | isplay/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | |
| **wcs3b-ls610d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-WCS3-020321/381 |
| **wcs3b-ls610d-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-WCS3-020321/382 |
| **wcs3b-ls610dh** | | | | | |
| Out-of- | 16-Feb-21 | 5 | A Denial of Service | https://cert. | H-PEP- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | WCS3-020321/383 |
| **wcs3b-ls610dh-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-WCS3-020321/384 |
| **wcs3b-ls610h** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006, https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vu | H-PEP-WCS3-020321/385 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | lnerability+in+PROFINET+IO+Device | |
| **wcs3b-ls610h-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 5 | A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.<br>**CVE ID : CVE-2021-20986** | https://cert.vde.com/en-us/advisories/vde-2021-006,<br>https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device | H-PEP-WCS3-020321/386 |
| **wcs3b-ls510** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007,<br>https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/387 |
| **wcs3b-ls510-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery. | https://cert.vde.com/en-us/advisories/vde-2021-007,<br>https://kb.hilscher.com/pages/viewpa | H-PEP-WCS3-020321/388 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-20987** | ge.action?pageId=108969480 | |
| **wcs3b-ls510d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/389 |
| **wcs3b-ls510d-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/390 |
| **wcs3b-ls510dh** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/391 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **wcs3b-ls510dh-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/392 |
| **wcs3b-ls510h** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/393 |
| **wcs3b-ls510h-om** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-WCS3-020321/394 |
| **pxv100-f200-b25-v1d** | | | | | |
| Out-of-bounds | 16-Feb-21 | 9 | A denial of service and memory corruption | https://cert.vde.com/en- | H-PEP-PXV1- |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | 020321/395 |
| **pxv100i-f200-b25-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-PXV1-020321/396 |
| **pcv100-f200-b25-v1d-6011-6720** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-PCV1-020321/397 |
| **pcv50-f200-b25-v1d** | | | | | |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may | https://cert.vde.com/en-us/advisories/vde-2021-007, | H-PEP-PCV5-020321/398 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
|  |  |  | lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 |  |
| **pcv80-f200-b25-v1d** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-PCV8-020321/399 |
| **pcv100-f200-b25-v1d-6011** |  |  |  |  |  |
| Out-of-bounds Write | 16-Feb-21 | 9 | A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.<br>**CVE ID : CVE-2021-20987** | https://cert.vde.com/en-us/advisories/vde-2021-007, https://kb.hilscher.com/pages/viewpage.action?pageId=108969480 | H-PEP-PCV1-020321/400 |
| **racom** |  |  |  |  |  |
| **m\!dge** |  |  |  |  |  |
| Exposure of Sensitive Information to an Unauthorized Actor | 16-Feb-21 | 5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to view sensitive syslog events without authentication.<br>**CVE ID : CVE-2021-20067** | N/A | H-RAC-M\!D-020321/401 |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **m\!dge_cellular_router** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the error handling functionality of web pages.<br>**CVE ID : CVE-2021-20068** | N/A | H-RAC-M\!D-020321/402 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the regionalSettings.php dialogs.<br>**CVE ID : CVE-2021-20069** | N/A | H-RAC-M\!D-020321/403 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the virtualization.php dialogs.<br>**CVE ID : CVE-2021-20070** | N/A | H-RAC-M\!D-020321/404 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-21 | 3.5 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the sms.php dialogs.<br>**CVE ID : CVE-2021-20071** | N/A | H-RAC-M\!D-020321/405 |
| Improper Privilege Management | 16-Feb-21 | 8.7 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to arbitrarily access and delete files via an authenticated directory traveral. | N/A | H-RAC-M\!D-020321/406 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2021-20072** | | |
| Cross-Site Request Forgery (CSRF) | 16-Feb-21 | 6.8 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows for cross-site request forgeries.<br>**CVE ID : CVE-2021-20073** | N/A | H-RAC-M\!D-020321/407 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 16-Feb-21 | 9 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows users to escape the provided command line interface and execute arbitrary OS commands.<br>**CVE ID : CVE-2021-20074** | N/A | H-RAC-M\!D-020321/408 |
| Improper Privilege Management | 16-Feb-21 | 7.2 | Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows for privilege escalation via configd.<br>**CVE ID : CVE-2021-20075** | N/A | H-RAC-M\!D-020321/409 |
| **se** | | | | | |
| **powerlogic_ion7400** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/410 |
| Cleartext Transmission of Sensitive | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability | https://www.se.com/ww/en/downl | H-SE-POWE-020321/411 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information | | | exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | oad/document/SEVD-2021-040-01/ | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/412 |
| **powerlogic_ion7410** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/413 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | | |
| **powerlogic_ion7650** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/414 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/415 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, | https://www.se.com/ww/en/download/document/SEVD-2021-040- | H-SE-POWE-020321/416 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | 01/ | |
| **powerlogic_ion8600** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/417 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/418 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/419 |
| **powerlogic_ion8650** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/420 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/421 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/422 |
| **powerlogic_ion8800** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/423 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic | https://www.se.com/ww/en/download/docume | H-SE-POWE-020321/424 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | nt/SEVD-2021-040-01/ | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/425 |
| **powerlogic_ion9000** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/426 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP web interface.<br>**CVE ID : CVE-2021-22701** | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/427 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/428 |
| **powerlogic_pm8000** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, | https://www.se.com/ww/en/download/document/SEVD- | H-SE-POWE-020321/429 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | 2021-040-01/ | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/430 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/431 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **powerlogic_ion8300** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/432 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/433 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/434 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | | |
| **powerlogic_ion8400** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/435 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/436 |
| Cleartext Transmission of Sensitive | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability | https://www.se.com/ww/en/downl | H-SE-POWE-020321/437 |

| 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 | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information | | | exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | oad/document/SEVD-2021-040-01/ | |
| **powerlogic_ion8500** | | | | | |
| Cross-Site Request Forgery (CSRF) | 19-Feb-21 | 3.5 | A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.<br>**CVE ID : CVE-2021-22701** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/438 |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/439 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.<br>**CVE ID : CVE-2021-22703** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/440 |
| **powerlogic_ion7700** | | | | | |
| Cleartext Transmission of Sensitive Information | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | https://www.se.com/ww/en/download/document/SEVD-2021-040-01/ | H-SE-POWE-020321/441 |
| **powerlogic_ion7300** | | | | | |
| Cleartext Transmissio | 19-Feb-21 | 5 | A CWE-319: Cleartext transmission of sensitive | https://www.se.com/w | H-SE-POWE-020321/442 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Sensitive Information | | | information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.<br>**CVE ID : CVE-2021-22702** | w/en/download/document/SEVD-2021-040-01/ | |
| **ui** | | | | | |
| **unifi_network_video_recorder** | | | | | |
| Uncontrolled Resource Consumption | 23-Feb-21 | 5 | UniFi Protect before v1.17.1 allows an attacker to use spoofed cameras to perform a denial-of-service attack that may cause the UniFi Protect controller to crash.<br>**CVE ID : CVE-2021-22882** | https://community.ui.com/releases/Security-advisory-bulletin-017-017/071141e5-bc2e-4b71-81f3-5e499316fcee | H-UI-UNIF-020321/443 |
| **unifi_cloud_key_plus** | | | | | |
| Uncontrolled Resource Consumption | 23-Feb-21 | 5 | UniFi Protect before v1.17.1 allows an attacker to use spoofed cameras to perform a denial-of-service attack that may cause the UniFi Protect controller to crash.<br>**CVE ID : CVE-2021-22882** | https://community.ui.com/releases/Security-advisory-bulletin-017-017/071141e5-bc2e-4b71-81f3-5e499316fcee | H-UI-UNIF-020321/444 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **unifi_dream_machine_pro** | | | | | |
| Uncontrolled Resource Consumption | 23-Feb-21 | 5 | UniFi Protect before v1.17.1 allows an attacker to use spoofed cameras to perform a denial-of-service attack that may cause the UniFi Protect controller to crash.<br>**CVE ID : CVE-2021-22882** | https://community.ui.com/releases/Security-advisory-bulletin-017-017/071141e5-bc2e-4b71-81f3-5e499316fcee | H-UI-UNIF-020321/445 |
| **yeastar** | | | | | |
| **neogate_tg400** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 19-Feb-21 | 4 | Yeastar NeoGate TG400 91.3.0.3 devices are affected by Directory Traversal. An authenticated user can decrypt firmware and can read sensitive information, such as a password or decryption key.<br>**CVE ID : CVE-2021-27328** | http://yeastar.com | H-YEA-NEOG-020321/446 |