| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Adobe** | | | | | |
| **after_effects** | | | | | |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | Adobe After Effects versions 22.1.1 (and earlier) and 18.4.3 (and earlier) are affected by an out-of-bounds write vulnerability 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-2022-23200** | https://helpx.adobe.com/security/products/after_effects/apsb22-09.html | A-ADO-AFTE-040322/1 |
| **commerce** | | | | | |
| Improper Input Validation | 16-Feb-22 | 10 | Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability during the checkout process. Exploitation of this issue does not require user interaction and could result in arbitrary code execution.<br>**CVE ID : CVE-2022-24086** | https://helpx.adobe.com/security/products/magento/apsb22-12.html | A-ADO-COMM-040322/2 |
| **creative_cloud_desktop_application** | | | | | |
| Uncontrolled Search Path Element | 16-Feb-22 | 5.1 | Adobe Creative Cloud Desktop version 2.7.0.13 (and earlier) is affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in | https://helpx.adobe.com/security/products/creative-cloud/apsb2 | A-ADO-CREA-040322/3 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the context of the current user. Exploitation of this issue requires user interaction in that a victim must download a malicious DLL file. The attacker has to deliver the DLL on the same folder as the installer which makes it as a high complexity attack vector.<br>**CVE ID : CVE-2022-23202** | 2-11.html | |
| **illustrator** | | | | | |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds write vulnerability 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-2022-23186** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/4 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 16-Feb-22 | 6.8 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted malicious file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted malicious file in Illustrator.<br>**CVE ID : CVE-2022-23188** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/5 |
| NULL Pointer | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 | https://helpx.adobe.com/s | A-ADO-ILLU- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Dereference | | | (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23189** | ecurity/products/illustrator/apsb22-07.html | 040322/6 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23190** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/7 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/8 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-23191** | | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23192** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/9 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23193** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/10 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/11 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23194** | | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23195** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/12 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23196** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/13 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/14 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23197** | | |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23198** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/15 |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23199** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | A-ADO-ILLU-040322/16 |
| **photoshop** | | | | | |
| Buffer Copy | 16-Feb-22 | 6.8 | Adobe Photoshop versions | https://helpx | A-ADO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| without Checking Size of Input ('Classic Buffer Overflow') | | | 22.5.4 (and earlier) and 23.1 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file in Photoshop.<br>**CVE ID : CVE-2022-23203** | .adobe.com/security/products/photoshop/apsb22-08.html | PHOT-040322/17 |
| **premiere_rush** | | | | | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Premiere Rush versions 2.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23204** | https://helpx.adobe.com/security/products/premiere_rush/apsb22-06.html | A-ADO-PREM-040322/18 |
| **ad_inserter_project** | | | | | |
| **ad_inserter** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Feb-22 | 4.3 | The Ad Inserter WordPress plugin before 2.7.10, Ad Inserter Pro WordPress plugin before 2.7.10 do not sanitise and escape the html_element_selection parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting | N/A | A-AD_-AD_I-040322/19 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-0288** | | |
| **ad_inserter_pro_project** | | | | | |
| **ad_inserter_pro** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Feb-22 | 4.3 | The Ad Inserter WordPress plugin before 2.7.10, Ad Inserter Pro WordPress plugin before 2.7.10 do not sanitise and escape the html_element_selection parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting<br>**CVE ID : CVE-2022-0288** | N/A | A-AD_-AD_I-040322/20 |
| **Airspan** | | | | | |
| **mimosa_management_platform** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | N/A | A-AIR-MIMO-040322/21 |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several | N/A | A-AIR-MIMO-040322/22 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | N/A | A-AIR-MIMO-040322/23 |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | N/A | A-AIR-MIMO-040322/24 |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some | N/A | A-AIR-MIMO-040322/25 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | | |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | A-AIR-MIMO-040322/26 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | N/A | A-AIR-MIMO-040322/27 |
| **alltube_project** | | | | | |
| **alltube** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| URL Redirection to Untrusted Site ('Open Redirect') | 21-Feb-22 | 5.8 | Open Redirect on Rudloff/alltube in Packagist rudloff/alltube prior to 3.0.1.<br>**CVE ID : CVE-2022-0692** | https://huntr.dev/bounties/4fb39400-e08b-47af-8c1f-5093c9a51203, https://github.com/rudloff/alltube/commit/bc14b6e45c766c05757fb607ef8d444cbbfba71a | A-ALL-ALLT-040322/28 |
| **alluxio** | | | | | |
| **alluxio** | | | | | |
| N/A | 20-Feb-22 | 7.5 | In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 Log4j vulnerability.<br>**CVE ID : CVE-2022-23848** | https://www.alluxio.io/download/releases/alluxio-2-7-3-release/ | A-ALL-ALLU-040322/29 |
| **BMC** | | | | | |
| **track-it\\!** | | | | | |
| Improper Authentication | 18-Feb-22 | 7.5 | This vulnerability allows remote attackers to bypass authentication on affected installations of BMC Track-It! 20.21.01.102. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to | https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It | A-BMC-TRAC-040322/30 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-14618.<br>**CVE ID : CVE-2022-24047** | | |
| **bologer** | | | | | |
| **anycomment** | | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 21-Feb-22 | 3.5 | The AnyComment WordPress plugin before 0.2.18 is affected by a race condition when liking/disliking a comment/reply, which could allow any authenticated user to quickly raise their rating or lower the rating of other users<br>**CVE ID : CVE-2022-0279** | N/A | A-BOL-ANYC-040322/31 |
| Cross-Site Request Forgery (CSRF) | 21-Feb-22 | 6.8 | The AnyComment WordPress plugin before 0.2.18 does not have CSRF checks in the Import and Revert HyperComments features, allowing attackers to make logged in admin perform such actions via a CSRF attack<br>**CVE ID : CVE-2022-0134** | N/A | A-BOL-ANYC-040322/32 |
| **brew** | | | | | |
| **mruby** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 16-Feb-22 | 4.3 | Use of Out-of-range Pointer Offset in Homebrew mruby prior to 3.2.<br>**CVE ID : CVE-2022-0614** | https://huntr.dev/bounties/a980ce4d-c359-4425-92c4-e844c0055879, https://github.com/mruby/mruby/co | A-BRE-MRUB-040322/33 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | mmit/ff3a5ebed6ffbe3e70481531cfb969b497aa73ad | |
| **bytecodealliance** | | | | | |
| **wasmtime** | | | | | |
| Access of Uninitialized Pointer | 16-Feb-22 | 7.1 | Wasmtime is an open source runtime for WebAssembly & WASI. Prior to versions 0.34.1 and 0.33.1, there exists a bug in the pooling instance allocator in Wasmtime's runtime where a failure to instantiate an instance for a module that defines an `externref` global will result in an invalid drop of a `VMExternRef` via an uninitialized pointer. A number of conditions listed in the GitHub Security Advisory must be true in order for an instance to be vulnerable to this issue. Maintainers believe that the effective impact of this bug is relatively small because the usage of `externref` is still uncommon and without a resource limiter configured on the `Store`, which is not the default configuration, it is only possible to trigger the bug from an error returned by `mprotect` or `VirtualAlloc`. Note that on Linux with the `uffd` feature enabled, it is only possible to trigger the bug from a resource limiter as | https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-88xq-w8cq-xfg7, https://github.com/bytecodealliance/wasmtime/commit/886ecc562040bef61faf19438c22285c2d62403a | A-BYT-WASM-040322/34 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the call to `mprotect` is skipped. The bug has been fixed in 0.34.1 and 0.33.1 and users are encouraged to upgrade as soon as possible. If it is not possible to upgrade to version 0.34.1 or 0.33.1 of the `wasmtime` crate, it is recommend that support for the reference types proposal be disabled by passing `false` to `Config::wasm_reference_types`. Doing so will prevent modules that use `externref` from being loaded entirely.<br>**CVE ID : CVE-2022-23636** | | |
| **cerebrate-project** | | | | | |
| **cerebrate** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-22 | 4.3 | An issue was discovered in Cerebrate through 1.4. genericForm allows reflected XSS in form descriptions via a user-controlled description.<br>**CVE ID : CVE-2022-25317** | https://github.com/cerebrate-project/cerebrate/commit/e60d97c214f9ac6df90c87241b3b3554afc06238 | A-CER-CERE-040322/35 |
| Exposure of Resource to Wrong Sphere | 18-Feb-22 | 4 | An issue was discovered in Cerebrate through 1.4. An incorrect sharing group ACL allowed an unprivileged user to edit and modify sharing groups.<br>**CVE ID : CVE-2022-25318** | https://github.com/cerebrate-project/cerebrate/commit/15190b930ebada9e8d294db57c96832799d9d93e | A-CER-CERE-040322/36 |
| N/A | 18-Feb-22 | 5 | An issue was discovered in Cerebrate through 1.4. | https://github.com/cerebr | A-CER-CERE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Endpoints could be open even when not enabled.<br>**CVE ID : CVE-2022-25319** | ate-project/cerebrate/commit/a2632349175e574cd6305fa459cd7610ea09ab61 | 040322/37 |
| N/A | 18-Feb-22 | 5 | An issue was discovered in Cerebrate through 1.4. Username enumeration could occur.<br>**CVE ID : CVE-2022-25320** | https://github.com/cerebrate-project/cerebrate/commit/88f3cc794486276a1f7e7331adb8ecb2dabd672f | A-CER-CERE-040322/38 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-22 | 4.3 | An issue was discovered in Cerebrate through 1.4. XSS could occur in the bookmarks component.<br>**CVE ID : CVE-2022-25321** | https://github.com/cerebrate-project/cerebrate/commit/e13b4e7bc5f1a0ff59b52162cc99405e89c0544a, https://github.com/cerebrate-project/cerebrate/commit/14ec995c2bd618b181197dc6b64e63fd966b4860 | A-CER-CERE-040322/39 |
| **Cesanta** | | | | | |
| **mongoose** | | | | | |
| Files or Directories Accessible to | 18-Feb-22 | 5 | This affects the package cesanta/mongoose before 7.6. The unsafe handling of file | https://snyk.io/vuln/SNYK- | A-CES-MONG-040322/40 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| External Parties | | | names during upload using mg_http_upload() method may enable attackers to write files to arbitrary locations outside the designated target folder.<br>**CVE ID : CVE-2022-25299** | UNMANAGED-CESANTAMONGOOSE-2404180, https://github.com/cesanta/mongoose/commit/c65c8fdaaa257e0487ab0aaae9e8f6b439335945 | |
| **Cisco** | | | | | |
| **evolved_programmable_network_manager** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Feb-22 | 4.3 | A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a 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. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-xss-P8fBz2FW | A-CIS-EVOL-040322/41 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20659** | | |
| **prime_infrastructure** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 17-Feb-22 | 4.3 | A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a 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-2022-20659** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-xss-P8fBz2FW | A-CIS-PRIM-040322/42 |
| **redundancy_configuration_manager** | | | | | |
| Improper Input Validation | 17-Feb-22 | 5 | A vulnerability in the checkpoint manager implementation of Cisco Redundancy Configuration Manager (RCM) for Cisco StarOS Software could allow an unauthenticated, remote attacker to cause the checkpoint manager process to restart upon receipt of | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-tcp-dos-2Wh8XjAQ | A-CIS-REDU-040322/43 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | malformed TCP data. This vulnerability is due to improper input validation of an ingress TCP packet. An attacker could exploit this vulnerability by sending crafted TCP data to the affected application. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the checkpoint manager process restarting.<br>**CVE ID : CVE-2022-20750** | | |
| **Coreftp** | | | | | |
| **core_ftp** | | | | | |
| Uncontrolled Resource Consumption | 17-Feb-22 | 2.6 | Core FTP / SFTP Server v2 Build 725 was discovered to allow unauthenticated attackers to cause a Denial of Service (DoS) via a crafted packet through the SSH service.<br>**CVE ID : CVE-2022-22899** | http://coreftp.com/forums/viewtopic.php?f=15&t=4022509 | A-COR-CORE-040322/44 |
| **Dart** | | | | | |
| **dart_software_development_kit** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 4 | Dart SDK contains the HTTPClient in dart:io library whcih includes authorization headers when handling cross origin redirects. These headers may be explicitly set and contain sensitive information. By default, HttpClient handles redirection logic. If a request is sent to example.com with authorization header and it | https://dart-review.googlesource.com/c/sdk/+/229947, https://github.com/dart-lang/sdk/commit/57db739be0ad4629079bfa94840064f615d35 | A-DAR-DART-040322/45 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | redirects to an attackers site, they might not expect attacker site to receive authorization header. We recommend updating the Dart SDK to version 2.16.0 or beyond.<br>**CVE ID : CVE-2022-0451** | abc | |
| **deliciousbrains** | | | | | |
| **database_backup** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 21-Feb-22 | 6.5 | The Database Backup for WordPress plugin before 2.5.1 does not properly sanitise and escape the fragment parameter before using it in a SQL statement in the admin dashboard, leading to a SQL injection issue<br>**CVE ID : CVE-2022-0255** | N/A | A-DEL-DATA-040322/46 |
| **drogon** | | | | | |
| **drogon** | | | | | |
| Files or Directories Accessible to External Parties | 21-Feb-22 | 6.5 | This affects the package drogonframework/drogon before 1.7.5. The unsafe handling of file names during upload using HttpFile::save() method may enable attackers to write files to arbitrary locations outside the designated target folder.<br>**CVE ID : CVE-2022-25297** | https://snyk.io/vuln/SNYK-UNMANAGED-DROGONFRAMEWORKDROGON-2407243, https://github.com/drogonframework/drogon/commit/3c785326c63a34aa1799a639ae185bc9453cb4 | A-DRO-DROG-040322/47 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 47, https://github.com/drogonframework/drogon/pull/1174 | |
| **Drupal** | | | | | |
| **drupal** | | | | | |
| Incorrect Authorization | 17-Feb-22 | 4 | The Quick Edit module does not properly check entity access in some circumstances. This could result in users with the "access in-place editing" permission viewing some content they are are not authorized to access. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed.<br>**CVE ID : CVE-2022-25270** | https://www.drupal.org/sa-core-2022-004 | A-DRU-DRUP-040322/48 |
| Improper Input Validation | 16-Feb-22 | 4.3 | Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.<br>**CVE ID : CVE-2022-25271** | https://www.drupal.org/sa-core-2022-003 | A-DRU-DRUP-040322/49 |
| **easycms** | | | | | |
| **easycms** | | | | | |
| Improper Neutralizatio | 16-Feb-22 | 7.5 | EasyCMS v1.6 allows for SQL injection via | N/A | A-EAS-EASY- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in an SQL Command ('SQL Injection') | | | ArticlemAction.class.php. In the background, search terms provided by the user were not sanitized and were used directly to construct a SQL statement.<br>**CVE ID : CVE-2022-23358** | | 040322/50 |
| **Eclipse** | | | | | |
| **lemminx** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 18-Feb-22 | 2.1 | A flaw was found in LemMinX in versions prior to 0.19.0. Insecure redirect could allow unauthorized access to sensitive information locally if LemMinX is run under a privileged user.<br>**CVE ID : CVE-2022-0672** | N/A | A-ECL-LEMM-040322/51 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-22 | 6.4 | A flaw was found in LemMinX in versions prior to 0.19.0. Cache poisoning of external schema files due to directory traversal.<br>**CVE ID : CVE-2022-0673** | N/A | A-ECL-LEMM-040322/52 |
| **filecloud** | | | | | |
| **filecloud** | | | | | |
| Cross-Site Request Forgery (CSRF) | 16-Feb-22 | 5.1 | In FileCloud before 21.3, the CSV user import functionality is vulnerable to Cross-Site Request Forgery (CSRF).<br>**CVE ID : CVE-2022-25241** | https://www.filecloud.com/supportdocs/display/cloud/Advisory+2022-01-3+Threat+of+CSRF+via+User+Creation | A-FIL-FILE-040322/53 |
| Cross-Site Request | 16-Feb-22 | 5.1 | In FileCloud before 21.3, file upload is not protected | https://www.filecloud.co | A-FIL-FILE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Forgery (CSRF) | | | against Cross-Site Request Forgery (CSRF).<br>**CVE ID : CVE-2022-25242** | m/supportdocs/display/cloud/Advisory+2022-01-2+Threat+of+CSRF+via+File+Upload | 040322/54 |
| **Foxit** | | | | | |
| **pdf_editor** | | | | | |
| Out-of-bounds Read | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader Foxit reader 11.0.1.0719 macOS. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the OnMouseExit method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14848.<br>**CVE ID : CVE-2022-24356** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/55 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/56 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15743.<br>**CVE ID : CVE-2022-24357** | | |
| Out-of-bounds Read | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15703.<br>**CVE ID : CVE-2022-24358** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/57 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF | https://www.foxit.com/support/security- | A-FOX-PDF_-040322/58 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15702.<br>**CVE ID : CVE-2022-24359** | bulletins.html | |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15744.<br>**CVE ID : CVE-2022-24360** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/59 |
| Out-of-bounds | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute | https://www.foxit.com/su | A-FOX-PDF_- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15811.<br>**CVE ID : CVE-2022-24361** | pport/security-bulletins.html | 040322/60 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15987. | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/61 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-24362** | | |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. Crafted data in a JP2 image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16087.<br>**CVE ID : CVE-2022-24369** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/62 |
| **pdf_reader** | | | | | |
| Out-of-bounds Read | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader Foxit reader 11.0.1.0719 macOS. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the OnMouseExit method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/63 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14848.<br>**CVE ID : CVE-2022-24356** | | |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15743.<br>**CVE ID : CVE-2022-24357** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/64 |
| Out-of-bounds Read | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. By performing actions in | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/65 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | JavaScript, an attacker can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15703.<br>**CVE ID : CVE-2022-24358** | | |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15702.<br>**CVE ID : CVE-2022-24359** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/66 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/67 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15744.<br>**CVE ID : CVE-2022-24360** | | |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15811.<br>**CVE ID : CVE-2022-24361** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/68 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/69 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | malicious page or open a malicious file. The specific flaw exists within the parsing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15987.<br>**CVE ID : CVE-2022-24362** | | |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. Crafted data in a JP2 image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16087.<br>**CVE ID : CVE-2022-24369** | https://www.foxit.com/support/security-bulletins.html | A-FOX-PDF_-040322/70 |
| **getshieldsecurity** | | | | | |
| **shield_security** | | | | | |
| Improper Neutralization of Input During Web | 21-Feb-22 | 3.5 | The Shield Security WordPress plugin before 13.0.6 does not sanitise and escape admin notes, which | N/A | A-GET-SHIE-040322/71 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Page Generation ('Cross-site Scripting') | | | could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.<br>**CVE ID : CVE-2022-0211** | | |
| **givewp** | | | | | |
| **givewp** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Feb-22 | 4.3 | The GiveWP WordPress plugin before 2.17.3 does not escape the json parameter before outputting it back in an attribute in the Import admin dashboard, leading to a Reflected Cross-Site Scripting<br>**CVE ID : CVE-2022-0252** | https://plugins.trac.wordpress.org/changeset/2659032 | A-GIV-GIVE-040322/72 |
| **gravitl** | | | | | |
| **netmaker** | | | | | |
| Use of Hard-coded Cryptographic Key | 18-Feb-22 | 10 | Use of Hard-coded Cryptographic Key in Go github.com/gravitl/netmaker prior to 0.8.5,0.9.4,0.10.0,0.10.1.<br>**CVE ID : CVE-2022-0664** | https://huntr.dev/bounties/29898a42-fd4f-4b5b-a8e3-ab573cb87eac, https://github.com/gravitl/netmaker/commit/9bee12642986cb9534e268447b70e6f0f03c59cf | A-GRA-NETM-040322/73 |
| **hashicorp** | | | | | |
| **nomad** | | | | | |
| N/A | 17-Feb-22 | 7.8 | HashiCorp Nomad and Nomad Enterprise 0.9.2 through | https://discuss.hashicorp. | A-HAS-NOMA- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 1.0.17, 1.1.11, and 1.2.5 allow operators with read-fs and alloc-exec (or job-submit) capabilities to read arbitrary files on the host filesystem as root.<br>**CVE ID : CVE-2022-24683** | com/t/hcsec-2022-02-nomad-alloc-filesystem-and-container-escape/35560, https://discuss.hashicorp.com | 040322/74 |
| **hospital_patient_record_management_system_project** | | | | | |
| **hospital_patient_record_management_system** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-22 | 3.5 | A stored cross-site scripting (XSS) vulnerability in Hospital Patient Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the Name field.<br>**CVE ID : CVE-2022-22853** | N/A | A-HOS-HOSP-040322/75 |
| **hutool** | | | | | |
| **hutool** | | | | | |
| Improper Certificate Validation | 16-Feb-22 | 7.5 | Hutool v5.7.18's HttpRequest was discovered to ignore all TLS/SSL certificate validation.<br>**CVE ID : CVE-2022-22885** | N/A | A-HUT-HUTO-040322/76 |
| **jeecg** | | | | | |
| **jeecg_boot** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command | 16-Feb-22 | 7.5 | Jeecg-boot v3.0 was discovered to contain a SQL injection vulnerability via the code parameter in /jeecg-boot/sys/user/queryUserByDepId.<br>**CVE ID : CVE-2022-22880** | N/A | A-JEE-JEEC-040322/77 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Feb-22 | 7.5 | Jeecg-boot v3.0 was discovered to contain a SQL injection vulnerability via the code parameter in /sys/user/queryUserComponentData. **CVE ID : CVE-2022-22881** | N/A | A-JEE-JEEC-040322/78 |
| **Jerryscript** | | | | | |
| **jerryscript** | | | | | |
| Reachable Assertion | 17-Feb-22 | 4.3 | There is an Assertion in 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at parser_parse_function_arguments in /js/js-parser.c of JerryScript commit a6ab5e9. **CVE ID : CVE-2022-22901** | https://github.com/jerryscript-project/jerryscript/issues/4916 | A-JER-JERR-040322/79 |
| **joinbookwyrm** | | | | | |
| **bookwyrm** | | | | | |
| Server-Side Request Forgery (SSRF) | 16-Feb-22 | 6.5 | BookWyrm is a decentralized social network for tracking reading habits and reviewing books. The functionality to load a cover via url is vulnerable to a server-side request forgery attack. Any BookWyrm instance running a version prior to v0.3.0 is susceptible to attack from a logged-in user. The problem has been patched and administrators should | https://github.com/bookwyrm-social/bookwyrm/security/advisories/GHSA-5m7g-66h6-5cvq | A-JOI-BOOK-040322/80 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | upgrade to version 0.3.0 As a workaround, BookWyrm instances can close registration and limit members to trusted individuals.<br>**CVE ID : CVE-2022-23644** | | |
| **jqueryform** | | | | | |
| **jqueryform** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-22 | 4.3 | A reflected cross-site scripting (XSS) vulnerability in forms generated by JQueryForm.com before 2022-02-05 allows remote attackers to inject arbitrary web script or HTML via the redirect parameter to admin.php.<br>**CVE ID : CVE-2022-24981** | https://JQueryForm.com | A-JQU-JQUE-040322/81 |
| Insufficiently Protected Credentials | 16-Feb-22 | 4 | Forms generated by JQueryForm.com before 2022-02-05 allows a remote authenticated attacker to access the cleartext credentials of all other form users. admin.php contains a hidden base64-encoded string with these credentials.<br>**CVE ID : CVE-2022-24982** | https://JQueryForm.com | A-JQU-JQUE-040322/82 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 16-Feb-22 | 5 | Forms generated by JQueryForm.com before 2022-02-05 allow remote attackers to obtain the URI to any uploaded file by capturing the POST response. When chained with CVE-2022-24984, this could lead to unauthenticated remote code | https://JQueryForm.com | A-JQU-JQUE-040322/83 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution on the underlying web server. This occurs because the Unique ID field is contained in the POST response upon submitting a form.<br>**CVE ID : CVE-2022-24983** | | |
| Unrestricted Upload of File with Dangerous Type | 16-Feb-22 | 6.8 | Forms generated by JQueryForm.com before 2022-02-05 (if file-upload capability is enabled) allow remote unauthenticated attackers to upload executable files and achieve remote code execution. This occurs because file-extension checks occur on the client side, and because not all executable content (e.g., .phtml or .php.bak) is blocked.<br>**CVE ID : CVE-2022-24984** | https://JQueryForm.com | A-JQU-JQUE-040322/84 |
| Improper Authentication | 16-Feb-22 | 6 | Forms generated by JQueryForm.com before 2022-02-05 allows a remote authenticated attacker to bypass authentication and access the administrative section of other forms hosted on the same web server. This is relevant only when an organization hosts more than one of these forms on their server.<br>**CVE ID : CVE-2022-24985** | https://JQueryForm.com | A-JQU-JQUE-040322/85 |
| **kicad** | | | | | |
| **eda** | | | | | |
| Out-of-bounds | 16-Feb-22 | 6.8 | A stack-based buffer overflow vulnerability exists in the | N/A | A-KIC-EDA-040322/86 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | Gerber Viewer gerber and excellon ReadXYCoord coordinate parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.<br>**CVE ID : CVE-2022-23803** | | |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon ReadIJCoord coordinate parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.<br>**CVE ID : CVE-2022-23804** | N/A | A-KIC-EDA-040322/87 |
| **libexpat_project** | | | | | |
| **libexpat** | | | | | |
| Improper Encoding or Escaping of Output | 16-Feb-22 | 7.5 | xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.<br>**CVE ID : CVE-2022-25235** | https://github.com/libexpat/libexpat/pull/562 | A-LIB-LIBE-040322/88 |
| Exposure of Resource to Wrong | 16-Feb-22 | 7.5 | xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert | https://github.com/libexpat/libexpat/p | A-LIB-LIBE-040322/89 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Sphere | | | namespace-separator characters into namespace URIs.<br>**CVE ID : CVE-2022-25236** | ull/561 | |
| Uncontrolled Resource Consumption | 18-Feb-22 | 4.3 | In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element.<br>**CVE ID : CVE-2022-25313** | N/A | A-LIB-LIBE-040322/90 |
| Integer Overflow or Wraparound | 18-Feb-22 | 5 | In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString.<br>**CVE ID : CVE-2022-25314** | N/A | A-LIB-LIBE-040322/91 |
| Integer Overflow or Wraparound | 18-Feb-22 | 7.5 | In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.<br>**CVE ID : CVE-2022-25315** | N/A | A-LIB-LIBE-040322/92 |
| **livehelperchat** | | | | | |
| **live_helper_chat** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 16-Feb-22 | 3.5 | Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.<br>**CVE ID : CVE-2022-0612** | https://huntr.dev/bounties/eadcf7d2-a479-4901-abcc-1505d3f1b32f, https://github.com/livehelperchat/livehelperchat/commit/4d4f1db1701f09177896a38e43fd0c693835f03b | A-LIV-LIVE-040322/93 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **machothemes** | | | | | |
| **image_photo_gallery_final_tiles_grid** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Feb-22 | 3.5 | The Image Photo Gallery Final Tiles Grid WordPress plugin before 3.5.3 does not sanitise and escape the Description field when editing a gallery, allowing users with a role as low as contributor to perform Cross-Site Scripting attacks against other users having access to the gallery dashboard<br>**CVE ID : CVE-2022-0186** | N/A | A-MAC-IMAG-040322/94 |
| **Magento** | | | | | |
| **magento** | | | | | |
| Improper Input Validation | 16-Feb-22 | 10 | Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability during the checkout process. Exploitation of this issue does not require user interaction and could result in arbitrary code execution.<br>**CVE ID : CVE-2022-24086** | https://helpx.adobe.com/security/products/magento/apsb22-12.html | A-MAG-MAGE-040322/95 |
| **Mariadb** | | | | | |
| **mariadb** | | | | | |
| Stack-based Buffer Overflow | 18-Feb-22 | 4.6 | MariaDB CONNECT Storage Engine Stack-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to | https://mariadb.com/kb/en/security/ | A-MAR-MARI-040322/96 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16191.<br>**CVE ID : CVE-2022-24048** | | |
| Use After Free | 18-Feb-22 | 4.6 | MariaDB CONNECT Storage Engine Use-After-Free Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16207.<br>**CVE ID : CVE-2022-24050** | https://mariadb.com/kb/en/security/ | A-MAR-MARI-040322/97 |
| Use of Externally- | 18-Feb-22 | 4.6 | MariaDB CONNECT Storage Engine Format String | https://mariadb.com/kb/ | A-MAR-MARI- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Controlled Format String | | | Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16193.<br>**CVE ID : CVE-2022-24051** | en/security/ | 040322/98 |
| Heap-based Buffer Overflow | 18-Feb-22 | 4.6 | MariaDB CONNECT Storage Engine Heap-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to | https://mariadb.com/kb/en/security/ | A-MAR-MARI-040322/99 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16190.<br>**CVE ID : CVE-2022-24052** | | |
| **Microweber** | | | | | |
| **microweber** | | | | | |
| Cross-Site Request Forgery (CSRF) | 17-Feb-22 | 4.3 | Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11.<br>**CVE ID : CVE-2022-0638** | https://github.com/microweber/microweber/commit/756096da1260f29ff6f4532234d93d8e41dd5aa8, https://huntr.dev/bounties/9d3d883c-d74c-4fe2-9978-a8e3d1ccf9f3 | A-MIC-MICR-040322/100 |
| Generation of Error Message Containing Sensitive Information | 18-Feb-22 | 5 | Generation of Error Message Containing Sensitive Information in Packagist microweber/microweber prior to 1.2.11.<br>**CVE ID : CVE-2022-0660** | https://huntr.dev/bounties/01fd2e0d-b8cf-487f-a16c-7b088ef3a291, https://github.com/microweber/microweber/commit/2417bd2eda2aa2868c1dad1abf62341f22bfc20a | A-MIC-MICR-040322/101 |
| Improper Neutralization of CRLF | 18-Feb-22 | 5 | CRLF Injection leads to Stack Trace Exposure due to lack of filtering at | https://github.com/microweber/micro | A-MIC-MICR-040322/102 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Sequences ('CRLF Injection') | | | https://demo.microweber.org / in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0666** | weber/commit/f0e338f1b7dc5ec9d99231f4ed3fa6245a5eb128, https://huntr.dev/bounties/7215afc7-9133-4749-8e8e-0569317dbd55 | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-22 | 4.3 | Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0678** | https://huntr.dev/bounties/d707137a-aace-44c5-b15c-1807035716c0, https://github.com/microweber/microweber/commit/2b8fa5aac31e51e2aca83c7ef5d1281ba2e755f8 | A-MIC-MICR-040322/103 |
| N/A | 20-Feb-22 | 4 | Business Logic Errors in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0688** | https://github.com/microweber/microweber/commit/a41f0fddaf08ff12b2b82506b1ca9490c93ab605, https://huntr.dev/bounties/051ec6d4-0b0a-41bf-9ded- | A-MIC-MICR-040322/104 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 27813037c9c9 | |
| N/A | 19-Feb-22 | 5 | Use multiple time the one-time coupon in Packagist microweber/microweber prior to 1.2.11.<br>**CVE ID : CVE-2022-0689** | https://github.com/microweber/microweber/commit/c3c25ae6c421bb4a65df9e0035edcc2f75594a04, https://huntr.dev/bounties/fa5dbbd3-97fe-41a9-8797-2e54d9a9c649 | A-MIC-MICR-040322/105 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 19-Feb-22 | 4.3 | Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.<br>**CVE ID : CVE-2022-0690** | https://github.com/microweber/microweber/commit/f7f5d41ba1a08ceed37c00d5f70a3f48b272e9f2, https://huntr.dev/bounties/4999a0f4-6efb-4681-b4ba-b36babc366f9 | A-MIC-MICR-040322/106 |
| **mobisoft_-_mobiplus_project** | | | | | |
| **mobisoft_-_mobiplus** | | | | | |
| N/A | 16-Feb-22 | 5 | MobiSoft - MobiPlus User Take Over and Improper Handling of url Parameters Attacker can navigate to specific url which will expose | N/A | A-MOB-MOBI-040322/107 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | all the users and password in clear text. http://IP/MobiPlusWeb/Handlers/MainHandler.ashx?MethodName=GridData&GridName=Users<br>**CVE ID : CVE-2022-22792** | | |
| **mruby** | | | | | |
| **mruby** | | | | | |
| Out-of-bounds Read | 17-Feb-22 | 6.4 | Out-of-bounds Read in Homebrew mruby prior to 3.2.<br>**CVE ID : CVE-2022-0623** | https://huntr.dev/bounties/5b908ac7-d8f1-4fcd-9355-85df565f7580, https://github.com/mruby/mruby/commit/ff3a5ebed6ffbe3e70481531cfb969b497aa73ad | A-MRU-MRUB-040322/108 |
| Out-of-bounds Read | 19-Feb-22 | 5.8 | Out-of-bounds Read in Homebrew mruby prior to 3.2.<br>**CVE ID : CVE-2022-0630** | https://github.com/mruby/mruby/commit/ff3a5ebed6ffbe3e70481531cfb969b497aa73ad, https://huntr.dev/bounties/f7cdd680-1a7f-4992-b4b8-44b5e4ba3e32 | A-MRU-MRUB-040322/109 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Heap-based Buffer Overflow | 18-Feb-22 | 7.5 | Heap-based Buffer Overflow in Homebrew mruby prior to 3.2.<br>**CVE ID : CVE-2022-0631** | https://github.com/mruby/mruby/commit/47068ae07a5fa3aa9a1879cdfe98a9ce0f339299, https://huntr.dev/bounties/9bdc49ca-6697-4adc-a785-081e1961bf40 | A-MRU-MRUB-040322/110 |
| NULL Pointer Dereference | 19-Feb-22 | 4.3 | NULL Pointer Dereference in Homebrew mruby prior to 3.2.<br>**CVE ID : CVE-2022-0632** | https://huntr.dev/bounties/3e5bb8f6-30fd-4553-86dd-761e9459ce1b, https://github.com/mruby/mruby/commit/44f591aa8f7091e6ca6cb418e428ae6d4ceaf77d | A-MRU-MRUB-040322/111 |
| **nasa** | | | | | |
| **openmct** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 20-Feb-22 | 3.5 | Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the “Condition Widget” element, that allows the injection of malicious JavaScript into the ‘URL’ field. This issue affects: nasa openmct 1.7.7 version and | https://github.com/nasa/openmct/commit/abc93d0ec4b104dac1ea5f8a615d06e3ab789 | A-NAS-OPEN-040322/112 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | prior versions; 1.3.0 version and later versions.<br>**CVE ID : CVE-2022-23053** | 34a | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Feb-22 | 3.5 | Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the "Summary Widget" element, that allows the injection of malicious JavaScript into the 'URL' field. This issue affects: nasa openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.<br>**CVE ID : CVE-2022-23054** | https://github.com/nasa/openmct/commit/abc93d0ec4b104dac1ea5f8a615d06e3ab78934a | A-NAS-OPEN-040322/113 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 20-Feb-22 | 3.5 | Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the "Web Page" element, that allows the injection of malicious JavaScript into the 'URL' field. This issue affects: nasa openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.<br>**CVE ID : CVE-2022-22126** | https://github.com/nasa/openmct/commit/abc93d0ec4b104dac1ea5f8a615d06e3ab78934a | A-NAS-OPEN-040322/114 |
| **Ovidentia** | | | | | |
| **ovidentia** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 17-Feb-22 | 5 | An incorrect access control issue in the component FileManager of Ovidentia CMS 6.0 allows authenticated attackers to to view and download content in the upload directory via path traversal.<br>**CVE ID : CVE-2022-22914** | N/A | A-OVI-OVID-040322/115 |
| **pcf2bdf_project** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **pcf2bdf** | | | | | |
| Out-of-bounds Write | 17-Feb-22 | 5.8 | A heap-buffer-overflow in pcf2bdf, versions >= 1.05 allows an attacker to trigger unsafe memory access via a specially crafted PCF font file. This out-of-bound read may lead to an application crash, information disclosure via program memory or other context-dependent impact. **CVE ID : CVE-2022-23318** | https://github.com/ganaware/pcf2bdf/issues/4 | A-PCF-PCF2-040322/116 |
| Uncontrolled Resource Consumption | 17-Feb-22 | 4.3 | A segmentation fault during PCF file parsing in pcf2bdf versions >=1.05 allows an attacker to trigger a program crash via a specially crafted PCF font file. This crash affects the availability of the software and dependent downstream components. **CVE ID : CVE-2022-23319** | https://github.com/ganaware/pcf2bdf/issues/5 | A-PCF-PCF2-040322/117 |
| **Pear** | | | | | |
| **crypt_gpg** | | | | | |
| Improper Input Validation | 17-Feb-22 | 5 | The Crypt_GPG extension before 1.6.7 for PHP does not prevent additional options in GPG calls, which presents a risk for certain environments and GPG versions. **CVE ID : CVE-2022-24953** | https://github.com/pear/Crypt_GPG/commit/29c0fbe96d0d4063ecd5c9a4644cb65a7fb7cc4e, https://github.com/pear/Crypt_GPG/commit/74c8f989cefbe0887274b461dc56197e121bf | A-PEA-CRYP-040322/118 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | d04 | |
| **php_everywhere_project** | | | | | |
| **php_everywhere** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 16-Feb-22 | 6.5 | PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via WordPress shortcodes, which can be used by any authenticated user.<br>**CVE ID : CVE-2022-24663** | N/A | A-PHP-PHP_-040322/119 |
| Improper Control of Generation of Code ('Code Injection') | 16-Feb-22 | 4 | PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via WordPress metaboxes, which could be used by any user able to edit posts.<br>**CVE ID : CVE-2022-24664** | N/A | A-PHP-PHP_-040322/120 |
| Improper Control of Generation of Code ('Code Injection') | 16-Feb-22 | 6.5 | PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via a WordPress gutenberg block by any user able to edit posts.<br>**CVE ID : CVE-2022-24665** | N/A | A-PHP-PHP_-040322/121 |
| **plist_project** | | | | | |
| **plist** | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 17-Feb-22 | 7.5 | Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution.<br>**CVE ID : CVE-2022-22912** | N/A | A-PLI-PLIS-040322/122 |
| **pluginus** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **woocs** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 21-Feb-22 | 4.3 | The WOOCS WordPress plugin before 1.3.7.5 does not sanitise and escape the woocs_in_order_currency parameter of the woocs_get_products_price_html AJAX action (available to both unauthenticated and authenticated users) before outputting it back in the response, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0234** | https://plugins.trac.wordpress.org/changeset/2659191 | A-PLU-WOOC-040322/123 |
| **prismjs** | | | | | |
| **prism** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-22 | 4.3 | Prism is a syntax highlighting library. Starting with version 1.14.0 and prior to version 1.27.0, Prism's command line plugin can be used by attackers to achieve a cross-site scripting attack. The command line plugin did not properly escape its output, leading to the input text being inserted into the DOM as HTML code. Server-side usage of Prism is not impacted. Websites that do not use the Command Line plugin are also not impacted. This bug has been fixed in v1.27.0. As a workaround, do not use the command line plugin on untrusted inputs, or sanitize all code blocks (remove all HTML code text) from all code blocks that use the command | https://github.com/PrismJS/prism/security/advisories/GHSA-3949-f494-cm99, https://github.com/PrismJS/prism/pull/3341, https://github.com/PrismJS/prism/commit/e002e78c343154e1c0ddf9d6a0bb85689e1a5c7c | A-PRI-PRIS-040322/124 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | line plugin.<br>**CVE ID : CVE-2022-23647** | | |
| **pritunl** | | | | | |
| **pritunl-client-electron** | | | | | |
| Improper Privilege Management | 20-Feb-22 | 4.6 | Pritunl Client through 1.2.3019.52 on Windows allows local privilege escalation, related to an ACL entry for CREATOR OWNER in platform_windows.go.<br>**CVE ID : CVE-2022-25372** | https://github.com/pritunl/pritunl-client-electron/commit/e16d47437f8ef62546aa00edb0d64be2a7d2205b | A-PRI-PRIT-040322/125 |
| **QT** | | | | | |
| **qt** | | | | | |
| N/A | 16-Feb-22 | 7.2 | In Qt 5.9.x through 5.15.x before 5.15.9 and 6.x before 6.2.4 on Linux and UNIX, QProcess could execute a binary from the current working directory when not found in the PATH.<br>**CVE ID : CVE-2022-25255** | https://download.qt.io/official_releases/qt/6.2/qprocess6-2.diff, https://codereview.qt-project.org/c/qt/qtbase/+/393113, https://download.qt.io/official_releases/qt/5.15/qprocess5-15.diff, https://codereview.qt-project.org/c/qt/qtbase/+/396020 | A-QT-QT-040322/126 |
| **quadlayers** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **perfect_brands_for_woocommerce** | | | | | |
| N/A | 18-Feb-22 | 4 | The vulnerability allows Subscriber+ level users to create brands in WordPress Perfect Brands for WooCommerce plugin (versions <= 2.0.4).<br>**CVE ID : CVE-2022-23981** | https://wordpress.org/plugins/perfect-woocommerce-brands/#developers, https://patchstack.com/database/vulnerability/perfect-woocommerce-brands/wordpress-perfect-brands-for-woocommerce-plugin-2-0-4-subscriber-set-featured-brand-vulnerability | A-QUA-PERF-040322/127 |
| Exposure of Sensitive Information to an Unauthorized Actor | 18-Feb-22 | 5 | The vulnerability discovered in WordPress Perfect Brands for WooCommerce plugin (versions <= 2.0.4) allows server information exposure.<br>**CVE ID : CVE-2022-23982** | https://wordpress.org/plugins/perfect-woocommerce-brands/#developers, https://patchstack.com/database/vulnerability/perfect-woocommerce-brands/word | A-QUA-PERF-040322/128 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | press-perfect-brands-for-woocommerce-plugin-2-0-4-server-information-exposure-vulnerability | |
| **Radare** | | | | | |
| **radare2** | | | | | |
| Use After Free | 16-Feb-22 | 7.5 | Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2.<br>**CVE ID : CVE-2022-0559** | https://github.com/radareorg/radare2/commit/b5cb90b28ec71fda3504da04e3cc94a362807f5e, https://huntr.dev/bounties/aa80adb7-e900-44a5-ad05-91f3ccdfc81e | A-RAD-RADA-040322/129 |
| **Redhat** | | | | | |
| **vscode-xml** | | | | | |
| Uncontrolled Resource Consumption | 18-Feb-22 | 6.4 | A flaw was found in vscode-xml in versions prior to 0.19.0. Schema download could lead to blind SSRF or DoS via a large file.<br>**CVE ID : CVE-2022-0671** | N/A | A-RED-VSCO-040322/130 |
| **rigoblock** | | | | | |
| **drago** | | | | | |
| Incorrect Permission Assignment | 18-Feb-22 | 5 | RigoBlock Dragos through 2022-02-17 lacks the onlyOwner modifier for | N/A | A-RIG-DRAG- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| for Critical Resource | | | setMultipleAllowances. This enables token manipulation, as exploited in the wild in February 2022. NOTE: although 2022-02-17 is the vendor's vulnerability announcement date, the vulnerability will not be remediated until a major protocol upgrade occurs.<br>**CVE ID : CVE-2022-25335** | | 040322/131 |
| **santesoft** | | | | | |
| **dicom_viewer_pro** | | | | | |
| Out-of-bounds Read | 18-Feb-22 | 4.3 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of GIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14972.<br>**CVE ID : CVE-2022-24055** | N/A | A-SAN-DICO-040322/132 |
| Out-of-bounds | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute | N/A | A-SAN-DICO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15076.<br>**CVE ID : CVE-2022-24056** | | 040322/133 |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15077.<br>**CVE ID : CVE-2022-24057** | N/A | A-SAN-DICO-040322/134 |
| Out-of-bounds | 18-Feb-22 | 9.3 | This vulnerability allows remote attackers to execute | N/A | A-SAN-DICO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15095.<br>**CVE ID : CVE-2022-24058** | | 040322/135 |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. Crafted data in a DCM file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-15098.<br>**CVE ID : CVE-2022-24059** | N/A | A-SAN-DICO-040322/136 |
| Out-of-bounds Read | 18-Feb-22 | 4.3 | This vulnerability allows remote attackers to disclose | N/A | A-SAN-DICO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sensitive information on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. Crafted data in a DCM file can trigger a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15099.<br>**CVE ID : CVE-2022-24060** | | 040322/137 |
| Use After Free | 18-Feb-22 | 4.3 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante DICOM Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15100. | N/A | A-SAN-DICO-040322/138 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-24061** | | |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 13.2.0.21165. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15104.<br>**CVE ID : CVE-2022-24062** | N/A | A-SAN-DICO-040322/139 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 13.2.0.21165. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code | N/A | A-SAN-DICO-040322/140 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in the context of the current process. Was ZDI-CAN-15105.<br>**CVE ID : CVE-2022-24063** | | |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.8.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15161.<br>**CVE ID : CVE-2022-24064** | N/A | A-SAN-DICO-040322/141 |
| **showdoc** | | | | | |
| **showdoc** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 19-Feb-22 | 6.8 | Unrestricted Upload of File with Dangerous Type in Packagist showdoc/showdoc prior to 2.10.2.<br>**CVE ID : CVE-2022-0409** | https://huntr.dev/bounties/c25bfad1-2611-4226-954f-009e50f966f7, https://github.com/star7th/showdoc/commit/7383d7a3c1b0807b6f397ba7df415a0ce7ccc | A-SHO-SHOW-040322/142 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 436 | |
| **snipeitapp** | | | | | |
| **snipe-it** | | | | | |
| Improper Privilege Management | 16-Feb-22 | 6.5 | Improper Privilege Management in Packagist snipe/snipe-it prior to 5.3.11. **CVE ID : CVE-2022-0611** | https://huntr.dev/bounties/7b7447fc-f1b0-446c-b016-ee3f6511010b, https://github.com/snipe/snipe-it/commit/321be4733d3997fc738f0118e1b9af5905f95439 | A-SNI-SNIP-040322/143 |
| Generation of Error Message Containing Sensitive Information | 17-Feb-22 | 5 | Generation of Error Message Containing Sensitive Information in Packagist snipe/snipe-it prior to 5.3.11. **CVE ID : CVE-2022-0622** | https://huntr.dev/bounties/4ed99dab-5319-4b6b-919a-84a9acd0061a, https://github.com/snipe/snipe-it/commit/178e44095141ab805c282f563fb088df1a10b2e2 | A-SNI-SNIP-040322/144 |
| **sygnoos** | | | | | |
| **popup_builder** | | | | | |
| Improper Neutralization of Special Elements | 21-Feb-22 | 6.5 | The Popup Builder WordPress plugin before 4.0.7 does not validate and properly escape the orderby and order | https://plugins.trac.wordpress.org/changeset/265 | A-SYG-POPU-040322/145 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an SQL Command ('SQL Injection') | | | parameters before using them in a SQL statement in the admin dashboard, which could allow high privilege users to perform SQL injection<br>**CVE ID : CVE-2022-0228** | 9117 | |
| **traefik** | | | | | |
| **traefik** | | | | | |
| Improper Certificate Validation | 17-Feb-22 | 6.8 | Traefik is an HTTP reverse proxy and load balancer. Prior to version 2.6.1, Traefik skips the router transport layer security (TLS) configuration when the host header is a fully qualified domain name (FQDN). For a request, the TLS configuration choice can be different than the router choice, which implies the use of a wrong TLS configuration. When sending a request using FQDN handled by a router configured with a dedicated TLS configuration, the TLS configuration falls back to the default configuration that might not correspond to the configured one. If the CNAME flattening is enabled, the selected TLS configuration is the SNI one and the routing uses the CNAME value, so this can skip the expected TLS configuration. Version 2.6.1 contains a patch for this issue. As a workaround, one may add the FDQN to the host rule. However, there is no workaround if the CNAME | https://github.com/traefik/traefik/security/advisories/GHSA-hrhx-6h34-j5hc, https://github.com/traefik/traefik/pull/8764 | A-TRA-TRAE-040322/146 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | flattening is enabled.<br>**CVE ID : CVE-2022-23632** | | |
| **updraftplus** | | | | | |
| **updraftplus** | | | | | |
| Incorrect Authorization | 17-Feb-22 | 4 | The UpdraftPlus WordPress plugin Free before 1.22.3 and Premium before 2.22.3 do not properly validate a user has the required privileges to access a backup's nonce identifier, which may allow any users with an account on the site (such as subscriber) to download the most recent site & database backup.<br>**CVE ID : CVE-2022-0633** | https://updraftplus.com/updraftplus-security-release-1-22-3-2-22-3/ | A-UPD-UPDR-040322/147 |
| **uri.js_project** | | | | | |
| **uri.js** | | | | | |
| Authorization Bypass Through User-Controlled Key | 16-Feb-22 | 6.4 | Authorization Bypass Through User-Controlled Key in NPM urijs prior to 1.19.8.<br>**CVE ID : CVE-2022-0613** | https://huntr.dev/bounties/f53d5c42-c108-40b8-917d-9dad51535083, https://github.com/medialize/uri.js/commit/6ea641cc8648b025ed5f30b090c2abd4d1a5249f | A-URI-URI.-040322/148 |
| **url-parse_project** | | | | | |
| **url-parse** | | | | | |
| Authorization Bypass | 17-Feb-22 | 5 | Authorization Bypass Through User-Controlled Key | https://github.com/unshif | A-URL-URL-- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Through User-Controlled Key | | | in NPM url-parse prior to 1.5.7.<br>**CVE ID : CVE-2022-0639** | tio/url-parse/commit/ef45a1355375a8244063793a19059b4f62fc8788, https://hunter.dev/bounties/83a6bc9a-b542-4a38-82cd-d995a1481155 | 040322/149 |
| Authorization Bypass Through User-Controlled Key | 21-Feb-22 | 7.5 | Authorization Bypass Through User-Controlled Key in NPM url-parse prior to 1.5.9.<br>**CVE ID : CVE-2022-0691** | https://github.com/unshiftio/url-parse/commit/0e3fb542d60ddbf6933f22eb9b1e06e25eaa5b63, https://hunter.dev/bounties/57124ed5-4b68-4934-8325-2c546257f2e4 | A-URL-URL--040322/150 |
| **vercel** | | | | | |
| **next.js** | | | | | |
| User Interface (UI) Misrepresentation of Critical Information | 17-Feb-22 | 4.3 | Next.js is a React framework. Starting with version 10.0.0 and prior to version 12.1.0, Next.js is vulnerable to User Interface (UI) Misrepresentation of Critical Information. In order to be affected, the `next.config.js` file must have an `images.domains` array | https://github.com/vercel/next.js/security/advisories/GHSA-fmvm-x8mv-47mj, https://github.com/vercel/next.js/pull | A-VER-NEXT-040322/151 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | assigned and the image host assigned in `images.domains` must allow user-provided SVG. If the `next.config.js` file has `images.loader` assigned to something other than default, the instance is not affected. Version 12.1.0 contains a patch for this issue. As a workaround, change `next.config.js` to use a different `loader configuration` other than the default.<br>**CVE ID : CVE-2022-23646** | /34075 | |
| **veronalabs** | | | | | |
| **wp_statistics** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 16-Feb-22 | 4.3 | The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the exclusion_reason parameter found in the ~/includes/class-wp-statistics-exclusion.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.4. This requires the "Record Exclusions" option to be enabled on the vulnerable site.<br>**CVE ID : CVE-2022-0513** | https://www.wordfence.com/blog/2022/02/unauthenticated-sql-injection-vulnerability-patched-in-wordpress-statistics-plugin/, https://plugins.trac.wordpress.org/changeset/2671297/wp-statistics/trunk/includes/class-wp-statistics-hits.php | A-VER-WP_S-040322/152 |
| **VIM** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **vim** | | | | | |
| Out-of-bounds Write | 17-Feb-22 | 6.8 | Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.<br>**CVE ID : CVE-2022-0629** | https://github.com/vim/vim/commit/34f8117dec685ace52cd9e578e2729db278163fc, https://huntr.dev/bounties/95e2b0da-e480-4ee8-9324-a93a2ab0a877 | A-VIM-VIM-040322/153 |
| N/A | 20-Feb-22 | 6.8 | Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4418.<br>**CVE ID : CVE-2022-0685** | https://huntr.dev/bounties/27230da3-9b1a-4d5d-8cdf-4b1e62fcd782, https://github.com/vim/vim/commit/5921aeb5741fc6e84c870d68c7c35b93ad0c9f87 | A-VIM-VIM-040322/154 |
| **Vmware** | | | | | |
| **cloud_foundation** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command | 16-Feb-22 | 7.2 | VMware NSX Edge contains a CLI shell injection vulnerability. A malicious actor with SSH access to an NSX-Edge appliance can execute arbitrary commands on the operating system as root. | https://www.vmware.com/security/advisories/VMSA-2022-0005.html | A-VMW-CLOU-040322/155 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | **CVE ID : CVE-2022-22945** | | |
| **nsx_data_center** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 16-Feb-22 | 7.2 | VMware NSX Edge contains a CLI shell injection vulnerability. A malicious actor with SSH access to an NSX-Edge appliance can execute arbitrary commands on the operating system as root.<br>**CVE ID : CVE-2022-22945** | https://www.vmware.com/security/advisories/VMSA-2022-0005.html | A-VMW-NSX_-040322/156 |
| **webcc_project** | | | | | |
| **webcc** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 18-Feb-22 | 5 | This affects the package sprinfall/webcc before 0.3.0. It is possible to traverse directories to fetch arbitrary files from the server.<br>**CVE ID : CVE-2022-25298** | https://snyk.io/vuln/SNYK-UNMANAGED-SPRINFALLWEBCC-2404182, https://github.com/sprinfall/webcc/commit/55a45fd5039061d5cc62e9f1b9d1f7e97a15143f | A-WEB-WEBC-040322/157 |
| **Wireshark** | | | | | |
| **wireshark** | | | | | |
| Excessive Iteration | 18-Feb-22 | 4.3 | Large loops in multiple protocol dissectors in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allow denial of service via packet injection or crafted capture file | https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0585.json, | A-WIR-WIRE-040322/158 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-0585** | https://www.wireshark.org/security/wnpa-sec-2022-02.html | |
| **wow-estore** | | | | | |
| **float_menu** | | | | | |
| Cross-Site Request Forgery (CSRF) | 21-Feb-22 | 4.3 | The Float menu WordPress plugin before 4.3.1 does not have CSRF check in place when deleting menu, which could allow attackers to make a logged in admin delete them via a CSRF attack<br>**CVE ID : CVE-2022-0313** | https://plugins.trac.wordpress.org/changeset/2661431 | A-WOW-FLOA-040322/159 |
| **wpdevart** | | | | | |
| **coming_soon_and_maintenance_mode** | | | | | |
| Incorrect Authorization | 21-Feb-22 | 4 | The Coming soon and Maintenance mode WordPress plugin before 3.6.8 does not have authorisation and CSRF checks in its coming_soon_send_mail AJAX action, allowing any authenticated users, with a role as low as subscriber to send arbitrary emails to all subscribed users<br>**CVE ID : CVE-2022-0164** | https://plugins.trac.wordpress.org/changeset/2655973 | A-WPD-COMI-040322/160 |
| Cross-Site Request Forgery (CSRF) | 21-Feb-22 | 4.3 | The Coming soon and Maintenance mode WordPress plugin before 3.6.8 does not have CSRF check in its coming_soon_send_mail AJAX action, allowing attackers to make logged in admin to send arbitrary | https://plugins.trac.wordpress.org/changeset/2659455 | A-WPD-COMI-040322/161 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | emails to all subscribed users via a CSRF attack<br>**CVE ID : CVE-2022-0199** | | |
| **zerof** | | | | | |
| **web_server** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-22 | 7.5 | ZEROF Web Server 2.0 allows /HandleEvent SQL Injection.<br>**CVE ID : CVE-2022-25322** | N/A | A-ZER-WEB_-040322/162 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 18-Feb-22 | 4.3 | ZEROF Web Server 2.0 allows /admin.back XSS.<br>**CVE ID : CVE-2022-25323** | N/A | A-ZER-WEB_-040322/163 |
| **zfaka_project** | | | | | |
| **zfaka** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 21-Feb-22 | 7.5 | An issue was found in Zfaka <= 1.4.5. The verification of the background file upload function check is not strict, resulting in remote command execution.<br>**CVE ID : CVE-2022-24553** | N/A | A-ZFA-ZFAK-040322/164 |
| **zoneland** | | | | | |
| **o2oa** | | | | | |
| N/A | 17-Feb-22 | 7.5 | O2OA v6.4.7 was discovered to contain a remote code execution (RCE) vulnerability via | N/A | A-ZON-O2OA-040322/165 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | /x_program_center/jaxrs/invoke.<br>**CVE ID : CVE-2022-22916** | | |
| **Hardware** | | | | | |
| **Airspan** | | | | | |
| **a5x** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | N/A | H-AIR-A5X-040322/166 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | H-AIR-A5X-040322/167 |
| Improper Neutralization of Special Elements used in an SQL | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly | N/A | H-AIR-A5X-040322/168 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('SQL Injection') | | | sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | N/A | H-AIR-A5X-040322/169 |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device | N/A | H-AIR-A5X-040322/170 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | | |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | H-AIR-A5X-040322/171 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | N/A | H-AIR-A5X-040322/172 |
| **c5c** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, | N/A | H-AIR-C5C-040322/173 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | H-AIR-C5C-040322/174 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | N/A | H-AIR-C5C-040322/175 |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive | N/A | H-AIR-C5C-040322/176 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information.<br>**CVE ID : CVE-2022-21196** | | |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | N/A | H-AIR-C5C-040322/177 |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | H-AIR-C5C-040322/178 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to | N/A | H-AIR-C5C-040322/179 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | | |
| **c5x** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | N/A | H-AIR-C5X-040322/180 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | H-AIR-C5X-040322/181 |
| Improper Neutralization of Special Elements | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: | N/A | H-AIR-C5X-040322/182 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an SQL Command ('SQL Injection') | | | Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | N/A | H-AIR-C5X-040322/183 |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions | N/A | H-AIR-C5X-040322/184 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | | |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | H-AIR-C5X-040322/185 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | N/A | H-AIR-C5X-040322/186 |
| **c6x** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve | N/A | H-AIR-C6X-040322/187 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | H-AIR-C6X-040322/188 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | N/A | H-AIR-C6X-040322/189 |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create | N/A | H-AIR-C6X-040322/190 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | | |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | N/A | H-AIR-C6X-040322/191 |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | H-AIR-C6X-040322/192 |
| Use of a Broken or Risky | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and | N/A | H-AIR-C6X-040322/193 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cryptographic Algorithm | | | PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | | |
| **totolink** | | | | | |
| **t10** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function updateWifiInfo of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25130** | N/A | H-TOT-T10-040322/194 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveCloudCheckStatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25131** | N/A | H-TOT-T10-040322/195 |
| Improper Neutralizatio | 19-Feb-22 | 7.5 | A command injection vulnerability in the function | N/A | H-TOT-T10-040322/196 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in a Command ('Command Injection') | | | meshSlaveDlfw of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25132** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function meshSlaveUpdate of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25136** | N/A | H-TOT-T10-040322/197 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveUpgstatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25137** | N/A | H-TOT-T10-040322/198 |
| **t6** | | | | | |
| Improper Neutralization of Special Elements used in a Command | 19-Feb-22 | 7.5 | A command injection vulnerability in the function updateWifiInfo of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B202110 | N/A | H-TOT-T6-040322/199 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Command Injection') | | | 15 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25130** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveCloudCheckStatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25131** | N/A | H-TOT-T6-040322/200 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function meshSlaveDlfw of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25132** | N/A | H-TOT-T6-040322/201 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function isAssocPriDevice of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25133** | N/A | H-TOT-T6-040322/202 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function setUpgradeFW of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25134** | N/A | H-TOT-T6-040322/203 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recv_mesh_info_sync of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25135** | N/A | H-TOT-T6-040322/204 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function meshSlaveUpdate of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25136** | N/A | H-TOT-T6-040322/205 |
| Improper Neutralization of Special Elements used in a Command ('Command | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveUpgstatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware | N/A | H-TOT-T6-040322/206 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25137** | | |
| **Tp-link** | | | | | |
| **ac1750** | | | | | |
| Integer Overflow or Wraparound | 18-Feb-22 | 8.3 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AC1750 prior to 1.1.4 Build 20211022 rel.59103(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko module. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15835.<br>**CVE ID : CVE-2022-24354** | N/A | H-TP--AC17-040322/207 |
| **tl-wa850re** | | | | | |
| Session Fixation | 18-Feb-22 | 7.5 | TP-Link TL-WA850RE Wi-Fi Range Extender before v6_200923 was discovered to use highly predictable and easily detectable session keys, allowing attackers to gain administrative privileges.<br>**CVE ID : CVE-2022-22922** | https://www.tp-link.com/us/support/download/tl-wa850re/v6/#Firmware | H-TP--TL-W-040322/208 |
| **tl-wr940n** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 18-Feb-22 | 8.3 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of file name extensions. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13910.<br>**CVE ID : CVE-2022-24355** | N/A | H-TP--TL-W-040322/209 |
| **Operating System** | | | | | |
| **Airspan** | | | | | |
| **a5x_firmware** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | N/A | O-AIR-A5X_-040322/210 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | O-AIR-A5X_-040322/211 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | N/A | O-AIR-A5X_-040322/212 |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | N/A | O-AIR-A5X_-040322/213 |
| Server-Side | 18-Feb-22 | 10 | This vulnerability could allow | N/A | O-AIR-A5X_- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Request Forgery (SSRF) | | | an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | | 040322/214 |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | O-AIR-A5X_-040322/215 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the | N/A | O-AIR-A5X_-040322/216 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | | |
| **c5c_firmware** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | N/A | O-AIR-C5C_-040322/217 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | O-AIR-C5C_-040322/218 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to | N/A | O-AIR-C5C_-040322/219 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | N/A | O-AIR-C5C_-040322/220 |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1. | N/A | O-AIR-C5C_-040322/221 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-21215** | | |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | O-AIR-C5C_-040322/222 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | N/A | O-AIR-C5C_-040322/223 |
| **c5x_firmware** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive | N/A | O-AIR-C5X_-040322/224 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information.<br>**CVE ID : CVE-2022-21141** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | O-AIR-C5X_-040322/225 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | N/A | O-AIR-C5X_-040322/226 |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information. | N/A | O-AIR-C5X_-040322/227 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-21196** | | |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | N/A | O-AIR-C5X_-040322/228 |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | O-AIR-C5X_-040322/229 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 | N/A | O-AIR-C5X_-040322/230 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | | |
| **c6x_firmware** | | | | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21141** | N/A | O-AIR-C6X_-040322/231 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.<br>**CVE ID : CVE-2022-21143** | N/A | O-AIR-C6X_-040322/232 |
| Improper Neutralization of Special Elements used in an | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to | N/A | O-AIR-C6X_-040322/233 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| SQL Command ('SQL Injection') | | | v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.<br>**CVE ID : CVE-2022-21176** | | |
| Incorrect Authorization | 18-Feb-22 | 10 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.<br>**CVE ID : CVE-2022-21196** | N/A | O-AIR-C6X_-040322/234 |
| Server-Side Request Forgery (SSRF) | 18-Feb-22 | 10 | This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C- | N/A | O-AIR-C6X_-040322/235 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | series and A5x: Device versions prior to v2.5.4.1.<br>**CVE ID : CVE-2022-21215** | | |
| Deserialization of Untrusted Data | 18-Feb-22 | 5 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.<br>**CVE ID : CVE-2022-0138** | N/A | O-AIR-C6X_-040322/236 |
| Use of a Broken or Risky Cryptographic Algorithm | 18-Feb-22 | 4 | MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.<br>**CVE ID : CVE-2022-21800** | N/A | O-AIR-C6X_-040322/237 |
| **Apple** | | | | | |
| **macos** | | | | | |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/238 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23186** | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 16-Feb-22 | 6.8 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted malicious file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted malicious file in Illustrator.<br>**CVE ID : CVE-2022-23188** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/239 |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23189** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/240 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/241 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23190** | | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23191** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/242 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23192** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/243 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read | https://helpx.adobe.com/security/products/illustrat | O-APP-MACO-040322/244 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23193** | or/apsb22-07.html | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23194** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/245 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23195** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/246 |
| Out-of- | 16-Feb-22 | 4.3 | Adobe Illustrator versions | https://helpx | O-APP- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Read | | | 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23196** | .adobe.com/security/products/illustrator/apsb22-07.html | MACO-040322/247 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23197** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/248 |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/249 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | malicious file.<br>**CVE ID : CVE-2022-23198** | | |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23199** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-APP-MACO-040322/250 |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | Adobe After Effects versions 22.1.1 (and earlier) and 18.4.3 (and earlier) are affected by an out-of-bounds write vulnerability 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-2022-23200** | https://helpx.adobe.com/security/products/after_effects/apsb22-09.html | O-APP-MACO-040322/251 |
| Out-of-bounds Read | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader Foxit reader 11.0.1.0719 macOS. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a | https://www.foxit.com/support/security-bulletins.html | O-APP-MACO-040322/252 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | malicious file. The specific flaw exists within the OnMouseExit method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14848.<br>**CVE ID : CVE-2022-24356** | | |
| **Cisco** | | | | | |
| **asyncos** | | | | | |
| N/A | 17-Feb-22 | 7.1 | A vulnerability in the DNS-based Authentication of Named Entities (DANE) email verification component of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient error handling in DNS name resolution by the affected software. An attacker could exploit this vulnerability by sending specially formatted email messages that are processed by an affected device. A successful exploit could allow the attacker to cause the device to become unreachable from management interfaces or to process additional email | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-MxZvGtgU | O-CIS-ASYN-040322/253 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | messages for a period of time until the device recovers, resulting in a DoS condition. Continued attacks could cause the device to become completely unavailable, resulting in a persistent DoS condition.<br>**CVE ID : CVE-2022-20653** | | |
| **Debian** | | | | | |
| **debian_linux** | | | | | |
| Improper Encoding or Escaping of Output | 16-Feb-22 | 7.5 | xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.<br>**CVE ID : CVE-2022-25235** | https://github.com/libexpat/libexpat/pull/562 | O-DEB-DEBI-040322/254 |
| Uncontrolled Resource Consumption | 18-Feb-22 | 4.3 | In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element.<br>**CVE ID : CVE-2022-25313** | N/A | O-DEB-DEBI-040322/255 |
| Integer Overflow or Wraparound | 18-Feb-22 | 5 | In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString.<br>**CVE ID : CVE-2022-25314** | N/A | O-DEB-DEBI-040322/256 |
| Integer Overflow or Wraparound | 18-Feb-22 | 7.5 | In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.<br>**CVE ID : CVE-2022-25315** | N/A | O-DEB-DEBI-040322/257 |
| **Fedoraproject** | | | | | |
| **fedora** | | | | | |
| NULL Pointer | 16-Feb-22 | 4.9 | An issue was discovered in drivers/usb/gadget/composit | https://github.com/torval | O-FED-FEDO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Dereference | | | e.c in the Linux kernel before 5.16.10. The USB Gadget subsystem lacks certain validation of interface OS descriptor requests (ones with a large array index and ones associated with NULL function pointer retrieval). Memory corruption might occur.<br>**CVE ID : CVE-2022-25258** | ds/linux/commit/75e5b4849b81e19e9efe1654b30d7f3151c33c2c, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.10 | 040322/258 |
| Out-of-bounds Write | 17-Feb-22 | 6.8 | Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.<br>**CVE ID : CVE-2022-0629** | https://github.com/vim/vim/commit/34f8117dec685ace52cd9e578e2729db278163fc, https://huntr.dev/bounties/95e2b0da-e480-4ee8-9324-a93a2ab0a877 | O-FED-FEDO-040322/259 |
| N/A | 20-Feb-22 | 6.8 | Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4418.<br>**CVE ID : CVE-2022-0685** | https://huntr.dev/bounties/27230da3-9b1a-4d5d-8cdf-4b1e62fcd782, https://github.com/vim/vim/commit/5921aeb5741fc6e84c870d68c7c35b93ad0c9f87 | O-FED-FEDO-040322/260 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Linux** | | | | | |
| **linux_kernel** | | | | | |
| N/A | 16-Feb-22 | 7.2 | In Qt 5.9.x through 5.15.x before 5.15.9 and 6.x before 6.2.4 on Linux and UNIX, QProcess could execute a binary from the current working directory when not found in the PATH.<br>**CVE ID : CVE-2022-25255** | https://download.qt.io/official_releases/qt/6.2/qprocess6-2.diff, https://codereview.qt-project.org/c/qt/qtbase/+/393113, https://download.qt.io/official_releases/qt/5.15/qprocess5-15.diff, https://codereview.qt-project.org/c/qt/qtbase/+/396020 | O-LIN-LINU-040322/261 |
| NULL Pointer Dereference | 16-Feb-22 | 4.9 | An issue was discovered in drivers/usb/gadget/composite.c in the Linux kernel before 5.16.10. The USB Gadget subsystem lacks certain validation of interface OS descriptor requests (ones with a large array index and ones associated with NULL function pointer retrieval). Memory corruption might occur.<br>**CVE ID : CVE-2022-25258** | https://github.com/torvalds/linux/commit/75e5b4849b81e19e9efe1654b30d7f3151c33c2c, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.10 | O-LIN-LINU-040322/262 |
| Improper Control of Dynamically- | 16-Feb-22 | 4.4 | In the Linux kernel through 5.16.10, certain binary files may have the exec-all | https://github.com/torvalds/linux/blo | O-LIN-LINU-040322/263 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Managed Code Resources | | | attribute if they were built in approximately 2003 (e.g., with GCC 3.2.2 and Linux kernel 2.4.20). This can cause execution of bytes located in supposedly non-executable regions of a file.<br>**CVE ID : CVE-2022-25265** | b/1c33bb0507508af24fd754dd7123bd8e997fab2f/arch/x86/include/asm/elf.h#L281-L294 | |
| Exposure of Resource to Wrong Sphere | 20-Feb-22 | 2.1 | An issue was discovered in drivers/usb/gadget/function/rndis.c in the Linux kernel before 5.16.10. The RNDIS USB gadget lacks validation of the size of the RNDIS_MSG_SET command. Attackers can obtain sensitive information from kernel memory.<br>**CVE ID : CVE-2022-25375** | https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.10, https://github.com/torvalds/linux/commit/38ea1eac7d88072bbffb630e2b3db83ca649b826, http://www.openwall.com/lists/oss-security/2022/02/21/1 | O-LIN-LINU-040322/264 |
| Use After Free | 18-Feb-22 | 7.2 | A flaw use after free in the Linux kernel Management Component Transport Protocol (MCTP) subsystem was found in the way user triggers cancel_work_sync after the unregister_netdev during removing device. A local user could use this flaw to crash the system or escalate their privileges on the system. It is actual from Linux Kernel 5.17-rc1 (when | https://lore.kernel.org/all/20220211011552.1861886-1-jk@codeconstruct.com.au | O-LIN-LINU-040322/265 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | mctp-serial.c introduced) till 5.17-rc5.<br>**CVE ID : CVE-2022-0646** | | |
| **Microsoft** | | | | | |
| **windows** | | | | | |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds write vulnerability 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-2022-23186** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/266 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 16-Feb-22 | 6.8 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted malicious file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted malicious file in Illustrator.<br>**CVE ID : CVE-2022-23188** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/267 |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/268 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability to achieve an application denial-of-service 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-2022-23189** | | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23190** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/269 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23191** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/270 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by | https://helpx.adobe.com/security/prod | O-MIC-WIND-040322/271 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23192** | ucts/illustrator/apsb22-07.html | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23193** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/272 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23194** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/273 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23195** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/274 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23196** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/275 |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/276 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | must open a malicious file.<br>**CVE ID : CVE-2022-23197** | | |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23198** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/277 |
| NULL Pointer Dereference | 16-Feb-22 | 4.3 | Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2022-23199** | https://helpx.adobe.com/security/products/illustrator/apsb22-07.html | O-MIC-WIND-040322/278 |
| Out-of-bounds Write | 16-Feb-22 | 6.8 | Adobe After Effects versions 22.1.1 (and earlier) and 18.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current | https://helpx.adobe.com/security/products/after_effects/apsb22-09.html | O-MIC-WIND-040322/279 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23200** | | |
| Out-of-bounds Read | 16-Feb-22 | 4.3 | Adobe Premiere Rush versions 2.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.<br>**CVE ID : CVE-2022-23204** | https://helpx.adobe.com/security/products/premiere_rush/apsb22-06.html | O-MIC-WIND-040322/280 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15743. | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/281 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-24357** | | |
| Out-of-bounds Read | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15703.<br>**CVE ID : CVE-2022-24358** | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/282 |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/283 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in the context of the current process. Was ZDI-CAN-15702.<br>**CVE ID : CVE-2022-24359** | | |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15744.<br>**CVE ID : CVE-2022-24360** | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/284 |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/285 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15811.<br>**CVE ID : CVE-2022-24361** | | |
| Use After Free | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15987.<br>**CVE ID : CVE-2022-24362** | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/286 |
| Out-of-bounds Write | 18-Feb-22 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. Crafted data in a JP2 image can trigger a | https://www.foxit.com/support/security-bulletins.html | O-MIC-WIND-040322/287 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16087.<br>**CVE ID : CVE-2022-24369** | | |
| Improper Privilege Management | 20-Feb-22 | 4.6 | Pritunl Client through 1.2.3019.52 on Windows allows local privilege escalation, related to an ACL entry for CREATOR OWNER in platform_windows.go.<br>**CVE ID : CVE-2022-25372** | https://github.com/pritunl/pritunl-client-electron/commit/e16d47437f8ef62546aa00edb0d64be2a7d2205b | O-MIC-WIND-040322/288 |
| **opengroup** | | | | | |
| **unix** | | | | | |
| N/A | 16-Feb-22 | 7.2 | In Qt 5.9.x through 5.15.x before 5.15.9 and 6.x before 6.2.4 on Linux and UNIX, QProcess could execute a binary from the current working directory when not found in the PATH.<br>**CVE ID : CVE-2022-25255** | https://download.qt.io/official_releases/qt/6.2/qprocess6-2.diff, https://codereview.qt-project.org/c/qt/qtbase/+/393113, https://download.qt.io/official_releases/qt/5.15/qprocess5-15.diff, https://codereview.qt-project.org/c/qt/qtbase/+ | O-OPE-UNIX-040322/289 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | /396020 | |
| **totolink** | | | | | |
| **t10_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function updateWifiInfo of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25130** | N/A | O-TOT-T10_-040322/290 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveCloudCheckStatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25131** | N/A | O-TOT-T10_-040322/291 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function meshSlaveDlfw of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25132** | N/A | O-TOT-T10_-040322/292 |
| Improper | 19-Feb-22 | 7.5 | A command injection | N/A | O-TOT- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Special Elements used in a Command ('Command Injection') | | | vulnerability in the function meshSlaveUpdate of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25136** | | T10_-040322/293 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveUpgstatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25137** | N/A | O-TOT-T10_-040322/294 |
| **t6_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function updateWifiInfo of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25130** | N/A | O-TOT-T6_F-040322/295 |
| Improper Neutralization of Special | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveCloudCheckStatus of | N/A | O-TOT-T6_F-040322/296 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in a Command ('Command Injection') | | | TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25131** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function meshSlaveDlfw of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25132** | N/A | O-TOT-T6_F-040322/297 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function isAssocPriDevice of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25133** | N/A | O-TOT-T6_F-040322/298 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function setUpgradeFW of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.<br>**CVE ID : CVE-2022-25134** | N/A | O-TOT-T6_F-040322/299 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recv_mesh_info_sync of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25135** | N/A | O-TOT-T6_F-040322/300 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function meshSlaveUpdate of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25136** | N/A | O-TOT-T6_F-040322/301 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 19-Feb-22 | 7.5 | A command injection vulnerability in the function recvSlaveUpgstatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet. **CVE ID : CVE-2022-25137** | N/A | O-TOT-T6_F-040322/302 |
| **Tp-link** | | | | | |
| **ac1750_firmware** | | | | | |
| Integer Overflow or | 18-Feb-22 | 8.3 | This vulnerability allows network-adjacent attackers to | N/A | O-TP--AC17-040322/303 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Wraparound | | | execute arbitrary code on affected installations of TP-Link AC1750 prior to 1.1.4 Build 20211022 rel.59103(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko module. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15835.<br>**CVE ID : CVE-2022-24354** | | |
| **tl-wa850re_firmware** | | | | | |
| Session Fixation | 18-Feb-22 | 7.5 | TP-Link TL-WA850RE Wi-Fi Range Extender before v6_200923 was discovered to use highly predictable and easily detectable session keys, allowing attackers to gain administrative privileges.<br>**CVE ID : CVE-2022-22922** | https://www.tp-link.com/us/support/download/tl-wa850re/v6/#Firmware | O-TP--TL-W-040322/304 |
| **tl-wr940n_firmware** | | | | | |
| Out-of-bounds Write | 18-Feb-22 | 8.3 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing | N/A | O-TP--TL-W-040322/305 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of file name extensions. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13910.<br>**CVE ID : CVE-2022-24355** | | |