National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 May 2022 Vol. 09 No. 09

## Table of Content

| Vendor | Product | Page Number |
|---|---|---|
| **Dlink** | mt6753 | 346 |
| | mt6755 | 349 |
| | mt6755s | 350 |
| | mt6757 | 351 |
| | mt6757c | 354 |
| | mt6757cd | 357 |
| | mt6757ch | 360 |
| | mt6758 | 363 |
| | mt6761 | 364 |
| | mt6762 | 373 |
| | mt6763 | 381 |
| | mt6765 | 384 |
| | mt6768 | 392 |
| | mt6769 | 401 |
| | mt6771 | 409 |
| | mt6779 | 418 |
| | mt6781 | 428 |
| | mt6785 | 437 |
| | mt6789 | 446 |
| | mt6795 | 451 |
| | mt6797 | 452 |
| | mt6799 | 454 |
| | mt6833 | 455 |
| | mt6853 | 465 |
| | mt6853t | 475 |
| | mt6873 | 484 |
| | mt6875 | 493 |
| | mt6877 | 502 |
| | mt6879 | 511 |
| | mt6883 | 517 |
| | mt6885 | 526 |
| | mt6889 | 536 |

| Vendor | Product | Page Number |
|---|---|---|
| **Dlink** | mt6891 | 544 |
| | mt6893 | 550 |
| | mt6895 | 560 |
| | mt6983 | 567 |
| | mt6985 | 573 |
| | mt8163 | 574 |
| | mt8167 | 580 |
| | mt8167s | 587 |
| | mt8168 | 587 |
| | mt8173 | 594 |
| | mt8175 | 602 |
| | mt8183 | 603 |
| | mt8185 | 604 |
| | mt8321 | 612 |
| | mt8362a | 620 |
| | mt8365 | 627 |
| | mt8385 | 635 |
| | mt8666 | 638 |
| | mt8667 | 641 |
| | mt8675 | 642 |
| | mt8695 | 645 |
| | mt8696 | 647 |
| | mt8735 | 651 |
| | mt8735b | 656 |
| | mt8765 | 661 |
| | mt8766 | 669 |
| | mt8768 | 677 |
| | mt8786 | 686 |
| | mt8788 | 695 |
| | mt8789 | 704 |
| | mt8791 | 713 |
| | mt8797 | 721 |

| Vendor | Product | Page Number |
|---|---|---|
| **Dlink** | mt9011 | 731 |
| | mt9215 | 732 |
| | mt9216 | 734 |
| | mt9220 | 736 |
| | mt9221 | 738 |
| | mt9255 | 739 |
| | mt9256 | 741 |
| | mt9266 | 743 |
| | mt9269 | 744 |
| | mt9285 | 746 |
| | mt9286 | 748 |
| | mt9288 | 750 |
| | mt9600 | 751 |
| | mt9602 | 753 |
| | mt9610 | 755 |
| | mt9611 | 756 |
| | mt9612 | 758 |
| | mt9613 | 760 |
| | mt9615 | 762 |
| | mt9617 | 763 |
| | mt9629 | 765 |
| | mt9630 | 767 |
| | mt9631 | 768 |
| | mt9632 | 770 |
| | mt9636 | 772 |
| | mt9638 | 774 |
| | mt9639 | 775 |
| | mt9650 | 777 |
| | mt9652 | 779 |
| | mt9666 | 780 |
| | mt9669 | 782 |
| | mt9670 | 784 |

# Common Vulnerabilities and Exposures (CVE) Report

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Vendor: 10web** | | | | | |
| **Product: photo_gallery** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible. **CVE ID : CVE-2022-1281** | https://plugins.trac.wordpress.org/changeset/2706797/photo-gallery/trunk/frontend/models/BWGModelGalleryBox.php?old=2587758&old_path=photo-gallery%2Ftrunk%2Ffrontend%2Fmodels%2FBWGModelGalleryBox.php | A-10W-PHOT-200522/1 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 6.1 | The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action. **CVE ID : CVE-2022-1282** | https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2706798%40photo-gallery&old=2694928%40photo-gallery&sfp_email=&sfph_mail= | A-10W-PHOT-200522/2 |
| **Vendor: Accusoft** | | | | | |
| **Product: imagegear** | | | | | |
| Incorrect Calculation of Buffer Size | 03-May-22 | 6.5 | A memory corruption vulnerability exists in the ioca_mys_rgb_allocat | N/A | A-ACC-IMAG-200522/3 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | e functionality of Accusoft ImageGear 19.10. A specially-crafted malformed file can lead to an arbitrary free. An attacker can provide a malicious file to trigger this vulnerability.<br>**CVE ID : CVE-2022-22137** | | |
| Out-of-bounds Write | 03-May-22 | 7.1 | A stack-based buffer overflow vulnerability exists in the IGXMPXMLParser::parseDelimiter functionality of Accusoft ImageGear 19.10. A specially-crafted PSD file can overflow a stack buffer, which could either lead to denial of service or, depending on the application, to an information leak. An attacker can provide a malicious file to trigger this vulnerability.<br>**CVE ID : CVE-2022-23400** | N/A | A-ACC-IMAG-200522/4 |
| **Vendor: acnam** | | | | | |
| **Product: ad_invalid_click_protector** | | | | | |
| Cross-Site Request Forgery (CSRF) | 02-May-22 | 6.5 | The Ad Invalid Click Protector (AICP) WordPress plugin before 1.2.7 does not have CSRF check | https://plugins.trac.wordpress.org/changeset/2705068 | A-ACN-AD_I-200522/5 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | deleting banned users, which could allow attackers to make a logged in admin remove arbitrary bans<br>**CVE ID : CVE-2022-0191** | | |
| **Vendor: Adobe** | | | | | |
| **Product: after_effects** | | | | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack 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 After Effects.<br>**CVE ID : CVE-2022-27783** | https://helpx.adobe.com/security/products/after_effects/apsb22-19.html | A-ADO-AFTE-200522/6 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code | https://helpx.adobe.com/security/products/after_effects/apsb22-19.html | A-ADO-AFTE-200522/7 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file in After Effects.<br>**CVE ID : CVE-2022-27784** | | |
| **Product: photoshop** | | | | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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-2022-23205** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/8 |
| Improper Input Validation | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an improper input validation vulnerability when parsing a PCX file that could result in arbitrary code execution in the | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/9 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious PCX file.<br>**CVE ID : CVE-2022-24098** | | |
| Out-of-bounds Read | 06-May-22 | 3.3 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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-2022-24099** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/10 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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. | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/11 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Exploitation of this issue requires user interaction in that a victim must open a malicious U3D file.<br>**CVE ID : CVE-2022-24105** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 SVG file.<br>**CVE ID : CVE-2022-28270** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/12 |
| Use After Free | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by a use-after-free 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 | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/13 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | victim must open a malicious PDF file.<br>**CVE ID : CVE-2022-28271** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28272** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/14 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28273** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/15 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2022-28274** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/16 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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. | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/17 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28275** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28276** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/18 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 PDF file.<br>**CVE ID : CVE-2022-28277** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | A-ADO-PHOT-200522/19 |
| **Vendor: ajdg** | | | | | |
| **Product: adrotate** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 4.8 | The AdRotate WordPress plugin before 5.8.23 does not escape Group Names, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed<br>**CVE ID : CVE-2022-0649** | N/A | A-AJD-ADRO-200522/20 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 4.8 | The AdRotate WordPress plugin before 5.8.23 does not sanitise and escape Advert Names which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed<br>**CVE ID : CVE-2022-0662** | N/A | A-AJD-ADRO-200522/21 |
| **Vendor: alibabagroup** | | | | | |
| **Product: one-java-agent** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 01-May-22 | 9.8 | All versions of package com.alibaba.oneagent:one-java-agent-plugin are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) using a specially crafted archive that | https://github.com/alibaba/one-java-agent/pull/29 | A-ALI-ONE--200522/22 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | holds directory traversal filenames (e.g. ../../evil.exe). The attacker can overwrite executable files and either invoke them remotely or wait for the system or user to call them, thus achieving remote command execution on the victim's machine.<br>**CVE ID : CVE-2022-25842** | | |
| **Vendor: angularjs** | | | | | |
| **Product: angular** | | | | | |
| Allocation of Resources Without Limits or Throttling | 01-May-22 | 7.5 | The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.<br>**CVE ID : CVE-2022-25844** | N/A | A-ANG-ANGU-200522/23 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: Apache** | | | | | |
| **Product: jena** | | | | | |
| Improper Restriction of XML External Entity Reference | 05-May-22 | 9.8 | A vulnerability in the RDF/XML parser of Apache Jena allows an attacker to cause an external DTD to be retrieved. This issue affects Apache Jena version 4.4.0 and prior versions. Apache Jena 4.2.x and 4.3.x do not allow external entities.<br>**CVE ID : CVE-2022-28890** | https://lists.apache.org/thread/h88oh642455wljo0p5jgzs9phk4gj878 | A-APA-JENA-200522/24 |
| **Vendor: ar-php** | | | | | |
| **Product: arphp** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | A reflected cross-site scripting (XSS) vulnerability in the component Query.php of arPHP v3.6.0 allows attackers to execute arbitrary web scripts.<br>**CVE ID : CVE-2022-28081** | N/A | A-AR--ARPH-200522/25 |
| **Vendor: bladex** | | | | | |
| **Product: springblade** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command | 05-May-22 | 9.8 | SpringBlade v3.2.0 and below was discovered to contain a SQL injection vulnerability via the component customSqlSegment. | N/A | A-BLA-SPRI-200522/26 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | **CVE ID : CVE-2022-27360** | | |
| **Vendor: bludit** | | | | | |
| **Product: bludit** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | A vulnerability was found in Bludit 3.13.1. It has been declared as problematic. This vulnerability affects the endpoint /admin/new-content of the New Content module. The manipulation of the argument content with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely but requires an authentication. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-1590** | N/A | A-BLU-BLUD-200522/27 |
| **Vendor: bluecms_project** | | | | | |
| **Product: bluecms** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command | 03-May-22 | 9.8 | Bluecms 1.6 has a SQL injection vulnerability at cooike. **CVE ID : CVE-2022-27962** | N/A | A-BLU-BLUE-200522/28 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('SQL Injection') | | | | | |
| **Vendor: bosscms** | | | | | |
| **Product: bosscms** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 05-May-22 | 9.8 | An arbitrary file upload vulnerability exists in Wenzhou Huoyin Information Technology Co., Ltd. BossCMS 1.0, which can be exploited by an attacker to gain control of the server. **CVE ID : CVE-2022-28606** | N/A | A-BOS-BOSS-200522/29 |
| **Vendor: Broadcom** | | | | | |
| **Product: sannav** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 06-May-22 | 9.8 | In Brocade SANnav before Brocade SANnav 2.2.0, multiple endpoints associated with Zone management are susceptible to SQL injection, allowing an attacker to run arbitrary SQL commands. **CVE ID : CVE-2022-28163** | https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-1842 | A-BRO-SANN-200522/30 |
| Inadequate Encryption Strength | 06-May-22 | 6.5 | Brocade SANnav before SANnav 2.2.0 application uses the Blowfish symmetric encryption algorithm for the storage of passwords. This could allow an authenticated attacker to decrypt | https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-1843 | A-BRO-SANN-200522/31 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | stored account passwords.<br>**CVE ID : CVE-2022-28164** | | |
| **Product: tcpreplay** | | | | | |
| Missing Release of Memory after Effective Lifetime | 04-May-22 | 7.5 | Tcpreplay version 4.4.1 contains a memory leakage flaw in fix_ipv6_checksums( ) function. The highest threat from this vulnerability is to data confidentiality.<br>**CVE ID : CVE-2022-28487** | https://github.com/appneta/tcpreplay/pull/720 | A-BRO-TCPR-200522/32 |
| **Vendor: chshcms** | | | | | |
| **Product: cscms** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 04-May-22 | 8.8 | Cscms 4.1 is vulnerable to SQL Injection. Log into the background, open the song module, create a new song, delete it to the recycle bin, and SQL injection security problems will occur when emptying the recycle bin.<br>**CVE ID : CVE-2022-28552** | N/A | A-CHS-CSCM-200522/33 |
| **Vendor: Cisco** | | | | | |
| **Product: enterprise_nfv_infrastructure_software** | | | | | |
| Incorrect Authorization | 04-May-22 | 9.9 | Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | A-CIS-ENTE-200522/34 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the root level, or leak system data from the host to the VM. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2022-20777** | sa-NFVIS-MUL-7DySRX9 | |
| Improper Input Validation | 04-May-22 | 8.8 | Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the root level, or leak system data from the host to the VM. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2022-20779** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9 | A-CIS-ENTE-200522/35 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Restriction of XML External Entity Reference | 04-May-22 | 7.4 | Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the root level, or leak system data from the host to the VM. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2022-20780** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9 | A-CIS-ENTE-200522/36 |
| **Product: firepower_management_center** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 5.4 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user- | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-qXz4uAkM | A-CIS-FIRE-200522/37 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.<br>**CVE ID : CVE-2022-20627** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 5.4 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-qXz4uAkM | A-CIS-FIRE-200522/38 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.<br>**CVE ID : CVE-2022-20628** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 5.4 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-qXz4uAkM | A-CIS-FIRE-200522/39 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.<br>**CVE ID : CVE-2022-20629** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 6.1 | A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by convincing a user to click a link designed to pass malicious input to the interface. A successful exploit could allow the attacker to conduct cross-site scripting | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-SfpEcvGT | A-CIS-FIRE-200522/40 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacks and gain access to sensitive browser-based information.<br>**CVE ID : CVE-2022-20740** | | |
| Unrestricted Upload of File with Dangerous Type | 03-May-22 | 8.8 | A vulnerability in the web management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to bypass security protections and upload malicious files to the affected system. This vulnerability is due to improper validation of files uploaded to the web management interface of Cisco FMC Software. An attacker could exploit this vulnerability by uploading a maliciously crafted file to a device running affected software. A successful exploit could allow the attacker to store malicious files on the device, which they could access later to conduct additional attacks, including | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-security-bypass-JhOd29Gg | A-CIS-FIRE-200522/41 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | executing arbitrary code on the affected device with root privileges.<br>**CVE ID : CVE-2022-20743** | | |
| Improper Input Validation | 03-May-22 | 6.5 | A vulnerability in the input protection mechanisms of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to view data without proper authorization. This vulnerability exists because of a protection mechanism that relies on the existence or values of a specific input. An attacker could exploit this vulnerability by modifying this input to bypass the protection mechanism and sending a crafted request to an affected device. A successful exploit could allow the attacker to view data beyond the scope of their authorization.<br>**CVE ID : CVE-2022-20744** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-infdisc-guJWRwQu | A-CIS-FIRE-200522/42 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: firepower_threat_defense** | | | | | |
| Improper Input Validation | 03-May-22 | 7.5 | A vulnerability in the remote access SSL VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper validation of errors that are logged as a result of client connections that are made using remote access VPN. An attacker could exploit this vulnerability by sending crafted requests to an affected system. A successful exploit could allow the attacker to cause the affected device to restart, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20715** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA | A-CIS-FIRE-200522/43 |
| XML Injection (aka Blind XPath Injection) | 03-May-22 | 7.8 | A vulnerability in CLI of Cisco Firepower Threat Defense (FTD) Software could allow an | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | A-CIS-FIRE-200522/44 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authenticated, local attacker to inject XML into the command parser. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted input in commands. A successful exploit could allow the attacker to inject XML into the command parser, which could result in unexpected processing of the command and unexpected command output.<br>**CVE ID : CVE-2022-20729** | sa-ftd-xmlinj-8GWjGzKe | |
| N/A | 03-May-22 | 7.5 | A vulnerability in the Security Intelligence feed feature of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the Security Intelligence DNS feed. This vulnerability is due to incorrect feed update processing. An attacker could exploit this vulnerability by sending traffic | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-sidns-bypass-3PzA5pO | A-CIS-FIRE-200522/45 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | through an affected device that should be blocked by the affected device. A successful exploit could allow the attacker to bypass device controls and successfully send traffic to devices that are expected to be protected by the affected device.<br>**CVE ID : CVE-2022-20730** | | |
| N/A | 03-May-22 | 7.4 | A vulnerability in an IPsec VPN library of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to read or modify data within an IPsec IKEv2 VPN tunnel. This vulnerability is due to an improper implementation of Galois/Counter Mode (GCM) ciphers. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a sufficient number of encrypted messages across an affected | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ipsec-mitm-CKnLr4 | A-CIS-FIRE-200522/46 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IPsec IKEv2 VPN tunnel and then using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to decrypt, read, modify, and re-encrypt data that is transmitted across an affected IPsec IKEv2 VPN tunnel.<br>**CVE ID : CVE-2022-20742** | | |
| Improper Input Validation | 03-May-22 | 7.5 | A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper input validation when parsing HTTPS requests. An attacker could exploit this vulnerability by sending a crafted HTTPS request to an affected device. A successful exploit could allow the | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-tzPSYern | A-CIS-FIRE-200522/47 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20745** | | |
| NULL Pointer Dereference | 03-May-22 | 7.5 | A vulnerability in the TCP proxy functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to improper handling of TCP flows. An attacker could exploit this vulnerability by sending a crafted stream of TCP traffic through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20746** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tcp-dos-kM9SHhOu | A-CIS-FIRE-200522/48 |
| Uncontrolled Resource Consumption | 03-May-22 | 5.3 | A vulnerability in the local malware analysis process of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-amp-local-dos-CUfwRJXT | A-CIS-FIRE-200522/49 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | cause a denial of service (DoS) condition on the affected device. This vulnerability is due to insufficient error handling in the local malware analysis process of an affected device. An attacker could exploit this vulnerability by sending a crafted file through the device. A successful exploit could allow the attacker to cause the local malware analysis process to crash, which could result in a DoS condition. Notes: Manual intervention may be required to recover from this situation. Malware cloud lookup and dynamic analysis will not be impacted.<br>**CVE ID : CVE-2022-20748** | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | A-CIS-FIRE-200522/50 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the connection handling function in Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-JnnJm4wB | A-CIS-FIRE-200522/51 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper traffic handling when platform limits are reached. An attacker could exploit this vulnerability by sending a high rate of UDP traffic through an affected device. A successful exploit could allow the attacker to cause all new, incoming connections to be dropped, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20757** | | |
| Improper Privilege Management | 03-May-22 | 8.8 | A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, but unprivileged, remote attacker to elevate privileges to level 15. This vulnerability is due to improper separation of authentication and | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye | A-CIS-FIRE-200522/52 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authorization scopes. An attacker could exploit this vulnerability by sending crafted HTTPS messages to the web services interface of an affected device. A successful exploit could allow the attacker to gain privilege level 15 access to the web management interface of the device. This includes privilege level 15 access to the device using management tools like the Cisco Adaptive Security Device Manager (ASDM) or the Cisco Security Manager (CSM). Note: With Cisco FTD Software, the impact is lower than the CVSS score suggests because the affected web management interface allows for read access only.<br>**CVE ID : CVE-2022-20759** | | |
| Uncontrolled Resource Consumption | 03-May-22 | 7.5 | A vulnerability in the DNS inspection handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-nJVAwOeq | A-CIS-FIRE-200522/53 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service condition (DoS) on an affected device. This vulnerability is due to a lack of proper processing of incoming requests. An attacker could exploit this vulnerability by sending crafted DNS requests at a high rate to an affected device. A successful exploit could allow the attacker to cause the device to stop responding, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20760** | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort rule evaluation function of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper handling of the DNS reputation | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FTD-snort3-DOS-Aq38LVdM | A-CIS-FIRE-200522/54 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | enforcement rule. An attacker could exploit this vulnerability by sending crafted UDP packets through an affected device to force a buildup of UDP connections. A successful exploit could allow the attacker to cause traffic that is going through the affected device to be dropped, resulting in a DoS condition. Note: This vulnerability only affects Cisco FTD devices that are running Snort 3.<br>**CVE ID : CVE-2022-20767** | | |
| **Product: sd-wan_vmanage** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 4.4 | A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, local attacker to view sensitive information on an affected system. This vulnerability is due to insufficient file system restrictions. An authenticated attacker with netadmin privileges could exploit this vulnerability by accessing the vshell | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmge-infodc-WPSkAMhp | A-CIS-SD-W-200522/55 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of an affected system. A successful exploit could allow the attacker to read sensitive information on the underlying operating system.<br>**CVE ID : CVE-2022-20734** | | |
| **Product: secure_endpoint** | | | | | |
| N/A | 04-May-22 | 7.5 | On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in CHM file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available. | N/A | A-CIS-SECU-200522/56 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20770** | | |
| N/A | 04-May-22 | 7.5 | On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in the TIFF file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available.<br>**CVE ID : CVE-2022-20771** | N/A | A-CIS-SECU-200522/57 |
| Missing Release of Memory after Effective Lifetime | 04-May-22 | 7.5 | On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was | N/A | A-CIS-SECU-200522/58 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosed: A vulnerability in HTML file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available.<br>**CVE ID : CVE-2022-20785** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-May-22 | 5.5 | On May 4, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in Clam AntiVirus (ClamAV) versions 0.103.4, 0.103.5, 0.104.1, and 0.104.2 could allow an authenticated, local attacker to cause a denial of service condition on | N/A | A-CIS-SECU-200522/59 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an affected device. For a description of this vulnerability, see the ClamAV blog.<br>**CVE ID : CVE-2022-20796** | | |
| **Product: telepresence_collaboration_endpoint** | | | | | |
| N/A | 04-May-22 | 8.1 | Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow a remote attacker to cause a denial of service (DoS) condition, view sensitive data on an affected device, or redirect users to an attacker-controlled destination. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2022-20764** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ROS-DOS-X7H7XhkK | A-CIS-TELE-200522/60 |
| URL Redirection to Untrusted Site ('Open Redirect') | 04-May-22 | 4.7 | Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow a remote attacker to cause a | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ROS-DOS-X7H7XhkK | A-CIS-TELE-200522/61 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | denial of service (DoS) condition, view sensitive data on an affected device, or redirect users to an attacker-controlled destination. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2022-20794** | | |
| **Vendor: Clamav** | | | | | |
| **Product: clamav** | | | | | |
| N/A | 04-May-22 | 7.5 | On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in CHM file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be | N/A | A-CLA-CLAM-200522/62 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | updated as additional information becomes available.<br>**CVE ID : CVE-2022-20770** | | |
| N/A | 04-May-22 | 7.5 | On April 20, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in the TIFF file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available.<br>**CVE ID : CVE-2022-20771** | N/A | A-CLA-CLAM-200522/63 |
| Missing Release of Memory after | 04-May-22 | 7.5 | On April 20, 2022, the following vulnerability in the ClamAV scanning | N/A | A-CLA-CLAM-200522/64 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Effective Lifetime | | | library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in HTML file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. This advisory will be updated as additional information becomes available. **CVE ID : CVE-2022-20785** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-May-22 | 5.5 | On May 4, 2022, the following vulnerability in the ClamAV scanning library versions 0.103.5 and earlier and 0.104.2 and earlier was disclosed: A vulnerability in Clam AntiVirus (ClamAV) versions 0.103.4, 0.103.5, 0.104.1, and 0.104.2 could allow | N/A | A-CLA-CLAM-200522/65 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an authenticated, local attacker to cause a denial of service condition on an affected device. For a description of this vulnerability, see the ClamAV blog. **CVE ID : CVE-2022-20796** | | |
| **Vendor: clinical-genomics** | | | | | |
| **Product: scout** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 7.5 | Path Traversal due to `send_file` call in GitHub repository clinical-genomics/scout prior to 4.52. **CVE ID : CVE-2022-1554** | https://github.com/clinical-genomics/scout/commit/952a2e2319af2d95d22b017a561730feac086ff1, https://huntr.dev/bounties/7acac778-5ba4-4f02-99e2-e4e17a81e600 | A-CLI-SCOU-200522/66 |
| Server-Side Request Forgery (SSRF) | 05-May-22 | 8.2 | Server-Side Request Forgery in scout in GitHub repository clinical-genomics/scout prior to v4.42. An attacker could make the application perform arbitrary requests to fishing steal cookie, request to private area, or lead to xss... **CVE ID : CVE-2022-1592** | https://huntr.dev/bounties/352b39da-0f2e-415a-9793-5480cae8bd27, https://github.com/clinical-genomics/scout/commit/b0ef15f4737d0c801154c1991b52ff5cab4f5c83 | A-CLI-SCOU-200522/67 |
| **Vendor: cloudways** | | | | | |
| **Product: breeze** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 02-May-22 | 5.4 | Plugin Settings Change leading to Cross-Site Scripting (XSS) vulnerability in Cloudways Breeze plugin <= 2.0.2 on WordPress allows users with a subscriber or higher user role to execute any of the wp_ajax_* actions in the class Breeze_Configuration which includes the ability to change any of the plugin's settings including CDN setting which could be further used for XSS attack.<br>**CVE ID : CVE-2022-29444** | https://patchstack.com/database/vulnerability/breeze/wordpress-breeze-plugin-2-0-2-plugin-settings-change-leading-to-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/breeze/#developers | A-CLO-BREE-200522/68 |
| **Vendor: Codection** | | | | | |
| **Product: import_and_export_users_and_customers** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 4.8 | The Import and export users and customers WordPress plugin before 1.19.2.1 does not sanitise and escaped imported CSV data, which could allow high privilege users to import malicious javascript code and lead to Stored Cross-Site Scripting issues<br>**CVE ID : CVE-2022-1255** | N/A | A-COD-IMPO-200522/69 |
| **Vendor: college_management_system_project** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: college_management_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-May-22 | 8.8 | College Management System v1.0 was discovered to contain a SQL injection vulnerability via the course_code parameter. **CVE ID : CVE-2022-28079** | N/A | A-COL-COLL-200522/70 |
| **Vendor: Contao** | | | | | |
| **Product: contao** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.1 | Cross-site Scripting (XSS) in GitHub repository contao/contao prior to 4.13.3. Attacker can execute Malicious JS in Application :) **CVE ID : CVE-2022-1588** | https://github.com/contao/contao/commit/199206849a87ddd0fa5cf674eb3c58292fd8366c, https://huntr.dev/bounties/df46e285-1b7f-403c-8f6c-8819e42deb80 | A-CON-CONT-200522/71 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-May-22 | 6.1 | Contao is a powerful open source CMS that allows you to create professional websites and scalable web applications. In versions of Contao prior to 4.13.3 it is possible to inject code into the canonical tag. As a workaround users may disable canonical tags in the root page settings. | https://github.com/contao/contao/security/advisories/GHSA-m8x6-6r63-qvj2, https://github.com/contao/contao/commit/199206849a87ddd0fa5cf674eb3c58292fd8366c, https://contao.org/en/security-advisories/cross-site-scripting- | A-CON-CONT-200522/72 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-24899** | via-canonical-url.html | |
| **Vendor: covid-19_directory_on_vaccination_system_project** | | | | | |
| **Product: covid-19_directory_on_vaccination_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-May-22 | 9.8 | Sourcecodester Covid-19 Directory on Vaccination System 1.0 is vulnerable to SQL Injection via cmdcategory. **CVE ID : CVE-2022-28530** | N/A | A-COV-COVI-200522/73 |
| **Vendor: csv-safe_project** | | | | | |
| **Product: csv-safe** | | | | | |
| Improper Neutralization of Formula Elements in a CSV File | 01-May-22 | 9.8 | CSV-Safe gem < 3.0.0 doesn't filter out special characters which could trigger CSV Injection. **CVE ID : CVE-2022-28481** | https://github.com/zvory/csv-safe/pull/8 | A-CSV-CSV--200522/74 |
| **Vendor: deltaww** | | | | | |
| **Product: diaenergie** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in HandlerChart.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/75 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execute system commands.<br>**CVE ID : CVE-2022-1366** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in Handler_TCV.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1367** | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/76 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in ReadRegIND. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1369** | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/77 |
| Improper Neutralization of Special Elements | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/78 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an SQL Command ('SQL Injection') | | | vulnerability exists in ReadREGbyID. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1370** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in ReadRegf. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1371** | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/79 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in dlSlog.aspx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands. | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/80 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-1372** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_unHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1374** | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/81 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_slogHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1375** | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/82 |
| Improper Neutralization of Special | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/83 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an SQL Command ('SQL Injection') | | | blind SQL injection vulnerability exists in DIAE_privgrpHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1376** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_rltHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1377** | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/84 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_pgHandler.ashx. This allows an attacker to inject arbitrary SQL | https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 | A-DEL-DIAE-200522/85 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | queries, retrieve and modify database contents, and execute system commands.<br>**CVE ID : CVE-2022-1378** | | |
| **Product: dmars** | | | | | |
| Improper Restriction of XML External Entity Reference | 03-May-22 | 5.5 | In four instances DMARS (All versions prior to v2.1.10.24) does not properly restrict references of XML external entities while processing specific project files, which may allow unauthorized information disclosure.<br>**CVE ID : CVE-2022-1331** | N/A | A-DEL-DMAR-200522/86 |
| **Vendor: dexie** | | | | | |
| **Product: dexie** | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 01-May-22 | 9.8 | The package dexie before 3.2.2, from 4.0.0-alpha.1 and before 4.0.0-alpha.3 are vulnerable to Prototype Pollution in the Dexie.setByKeyPath( obj, keyPath, value) function which does not properly check the keys being set (like __proto__ or constructor). This can allow an attacker to add/modify properties of the Object.prototype | https://github.com/dexie/Dexie.js/commit/1d655a69b9f28c3af6fae10cf5c61df387dc689b | A-DEX-DEXI-200522/87 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | leading to prototype pollution vulnerability. **Note:** This vulnerability can occur in multiple ways, for example when modifying a collection with untrusted user input. **CVE ID : CVE-2022-21189** | | |
| **Vendor: diagrams** | | | | | |
| **Product: drawio** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 9.6 | Arbitrary Code Execution through Sanitizer Bypass in GitHub repository jgraph/drawio prior to 18.0.0. - Arbitrary (remote) code execution in the desktop app. - Stored XSS in the web app. **CVE ID : CVE-2022-1575** | https://github.com/jgraph/drawio/commit/f768ed73875d5eca20110b9c1d72f2789cd1bab7, https://huntr.dev/bounties/033d3423-eb05-4b53-a747-1bfcba873127 | A-DIA-DRAW-200522/88 |
| **Vendor: documentor_project** | | | | | |
| **Product: documentor** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | The Documentor WordPress plugin through 1.5.3 fails to sanitize and escape user input before it is being interpolated in an SQL statement and then executed, leading to an SQL Injection exploitable by unauthenticated users. | N/A | A-DOC-DOCU-200522/89 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-0773** | | |
| **Vendor: dset_project** | | | | | |
| **Product: dset** | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 01-May-22 | 8.1 | All versions of package dset are vulnerable to Prototype Pollution via 'dset/merge' mode, as the dset function checks for prototype pollution by validating if the top-level path contains __proto__, constructor or protorype. By crafting a malicious object, it is possible to bypass this check and achieve prototype pollution.<br>**CVE ID : CVE-2022-25645** | N/A | A-DSE-DSET-200522/90 |
| **Vendor: e-commerce_website_project** | | | | | |
| **Product: e-commerce_website** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 5.4 | A cross-site scripting (XSS) vulnerability in /public/admin/index.php?add_product of E-Commerce Website v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Title text field.<br>**CVE ID : CVE-2022-27330** | N/A | A-E-C-E-CO-200522/91 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: edmonsoft** | | | | | |
| **Product: countdown_builder** | | | | | |
| Incorrect Authorization | 06-May-22 | 9.8 | Pro Features Lock Bypass vulnerability in Countdown & Clock plugin <= 2.3.2 at WordPress.<br>**CVE ID : CVE-2022-29423** | https://wordpress.org/plugins/countdown-builder/#developers, https://patchstack.com/database/vulnerability/countdown-builder/wordpress-countdown-clock-plugin-2-3-0-pro-features-lock-bypass-vulnerability | A-EDM-COUN-200522/92 |
| **Vendor: eve-ng** | | | | | |
| **Product: eve-ng** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-May-22 | 8.8 | An OS Command Injection vulnerability in the configuration parser of Eve-NG Professional through 4.0.1-65 and Eve-NG Community through 2.0.3-112 allows a remote authenticated attacker to execute commands as root by editing virtualization command parameters of imported UNL files.<br>**CVE ID : CVE-2022-27903** | https://www.eve-ng.net/, https://www.eve-ng.net/index.php/documentation/release-notes/ | A-EVE-EVE--200522/93 |
| **Vendor: event_list_project** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: event_list** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 4.8 | The Event List WordPress plugin before 0.8.8 does not sanitise and escape some of its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks against other admin even when the unfiltered_html is disallowed **CVE ID : CVE-2022-0418** | N/A | A-EVE-EVEN-200522/94 |
| **Vendor: event_management_system_project** | | | | | |
| **Product: event_management_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-May-22 | 8.8 | Royal Event Management System v1.0 was discovered to contain a SQL injection vulnerability via the todate parameter. **CVE ID : CVE-2022-28080** | N/A | A-EVE-EVEN-200522/95 |
| **Vendor: exfat_project** | | | | | |
| **Product: exfat** | | | | | |
| Allocation of Resources Without Limits or Throttling | 02-May-22 | 4.7 | relan exFAT 1.3.0 allows local users to obtain sensitive information (data from deleted files in the filesystem) in certain situations involving offsets beyond ValidDataLength. | N/A | A-EXF-EXFA-200522/96 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-29973** | | |
| **Vendor: experian** | | | | | |
| **Product: hunter** | | | | | |
| N/A | 04-May-22 | 4.3 | Experian Hunter 1.16 allows remote authenticated users to modify assumed-immutable elements via the (1) rule name parameter to the Rules page or the (2) subrule name or (3) categories name parameter to the Subrules page.<br>**CVE ID : CVE-2022-29950** | https://www.experian.in/hunter | A-EXP-HUNT-200522/97 |
| **Vendor: F5** | | | | | |
| **Product: access_for_android** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 05-May-22 | 5.5 | On F5 Access for Android 3.x versions prior to 3.0.8, a Task Hijacking vulnerability exists in the F5 Access for Android application, which may allow an attacker to steal sensitive user information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27875** | https://support.f5.com/csp/article/K40019131 | A-F5-ACCE-200522/98 |
| **Product: access_policy_manager_clients** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 7.8 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, the BIG-IP Edge Client Component Installer Service does not use best practice while saving temporary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29263** | https://support.f5.com/csp/article/K33552735 | A-F5-ACCE-200522/99 |
| **Product: big-ip_access_policy_manager** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/100 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/101 |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/102 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/103 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/104 |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/105 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/106 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Always-Incorrect Control Flow Implementation | 05-May-22 | 7.5 | On F5 BIG-IP Advanced WAF, ASM, and APM 16.1.x versions prior to 16.1.2.1, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when ASM or Advanced WAF, as well as APM, are configured on a virtual server, the ASM policy is configured with Session Awareness, and the "Use APM Username and Session ID" option is enabled, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26890** | https://support.f5.com/csp/article/K03442392 | A-F5-BIG--200522/107 |
| Uncontrolled Resource | 05-May-22 | 5.3 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K93543114 | A-F5-BIG--200522/108 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when APM is configured on a virtual server and the associated access profile is configured with APM AAA NTLM Auth, undisclosed requests can cause an increase in internal resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27181** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/109 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | | |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/110 |
| Improper Neutralization of Input During Web Page Generation | 05-May-22 | 6.1 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP APM, and F5 BIG-IP Guided Configuration (GC) all versions prior to | https://support.f5.com/csp/article/K21317311 | A-F5-BIG--200522/111 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | 9.0, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of F5 BIG-IP Guided Configuration that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27230** | | |
| Improper Input Validation | 05-May-22 | 7.2 | On 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, BIG-IP APM does not properly validate configurations, allowing an authenticated attacker with high privileges to manipulate the APM policy leading to privilege escalation/remote code execution. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27634** | https://support.f5.com/csp/article/K57555833 | A-F5-BIG--200522/112 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Insertion of Sensitive Information into Log File | 05-May-22 | 5.5 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, BIG-IP Edge Client may log sensitive APM session-related information when VPN is launched on a Windows system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-27636** | https://support.f5.com/csp/article/K57110035 | A-F5-BIG--200522/113 |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/114 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 7.2 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing command injection vulnerabilities in undisclosed URIs in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27806** | https://support.f5.com/csp/article/K68647001 | A-F5-BIG--200522/115 |
| Improper Neutralization of Input During | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/116 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/117 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/118 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/119 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/120 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/121 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/122 |
| Uncontrolled Search | 05-May-22 | 7.8 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K54460845 | A-F5-BIG--200522/123 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Path Element | | | 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, a DLL Hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28714** | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/124 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 7.8 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, the BIG-IP Edge Client Component Installer Service does not use best practice while saving temporary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29263** | https://support.f5.com/csp/article/K33552735 | A-F5-BIG--200522/125 |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/126 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/127 |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/128 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/129 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NULL Pointer Dereference | 05-May-22 | 7.5 | On F5 BIG-IP LTM, Advanced WAF, ASM, or APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a virtual server is configured with HTTP, TCP on one side (client/server), and DTLS on the other (server/client), undisclosed requests can cause the TMM process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29491** | https://support.f5.com/csp/article/K14229426 | A-F5-BIG--200522/130 |
| **Product: big-ip_access_policy_manager_client** | | | | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 5.5 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions | https://support.f5.com/csp/article/K57110035 | A-F5-BIG--200522/131 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | prior to 7.2.1.5, BIG-IP Edge Client may log sensitive APM session-related information when VPN is launched on a Windows system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27636** | | |
| Uncontrolled Search Path Element | 05-May-22 | 7.8 | On F5 BIG-IP APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, as well as F5 BIG-IP APM Clients 7.x versions prior to 7.2.1.5, a DLL Hijacking vulnerability exists in the BIG-IP Edge Client Windows Installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28714** | https://support.f5.com/csp/article/K54460845 | A-F5-BIG--200522/132 |
| **Product: big-ip_advanced_firewall_manager** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/133 |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/134 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | | |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/135 |
| Uncontrolled Resource | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/136 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/137 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | | |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/138 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/139 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/140 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-27182** | | |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/141 |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/142 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/143 |
| Uncontrolled Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/144 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Unrestricted Upload of File with Dangerous Type | 05-May-22 | 7.2 | On F5 BIG-IP AFM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, an authenticated attacker with high privileges can upload a maliciously crafted file to the BIG-IP AFM Configuration utility, which allows an attacker to run arbitrary commands. Note: Software versions which have | https://support.f5.com/csp/article/K08510472 | A-F5-BIG--200522/145 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28695** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/146 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/147 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/148 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/149 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/150 |
| Improper Neutralization of Input | 05-May-22 | 8.8 | On 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x | https://support.f5.com/csp/article/K25451853 | A-F5-BIG--200522/151 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x 11.6.x, a DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP AFM, CGNAT, and PEM Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28716** | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/152 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28859** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/153 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/154 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/155 |
| Uncontrolled Resource | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/156 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | | |
| **Product: big-ip_advanced_web_application_firewall** | | | | | |
| Always-Incorrect Control Flow Implementation | 05-May-22 | 7.5 | On F5 BIG-IP Advanced WAF, ASM, and APM 16.1.x versions prior to 16.1.2.1, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when ASM or Advanced WAF, as well as APM, are configured on a virtual server, the ASM policy is configured with Session Awareness, and the "Use APM Username and Session ID" option is enabled, undisclosed requests can cause the bd process to terminate. Note: Software versions | https://support.f5.com/csp/article/K03442392 | A-F5-BIG--200522/157 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26890** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 7.2 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing command injection vulnerabilities in undisclosed URIs in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27806** | https://support.f5.com/csp/article/K68647001 | A-F5-BIG--200522/158 |
| NULL Pointer Dereference | 05-May-22 | 7.5 | On F5 BIG-IP LTM, Advanced WAF, ASM, or APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x | https://support.f5.com/csp/article/K14229426 | A-F5-BIG--200522/159 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions prior to 14.1.4.6, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a virtual server is configured with HTTP, TCP on one side (client/server), and DTLS on the other (server/client), undisclosed requests can cause the TMM process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29491** | | |
| **Product: big-ip_analytics** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/160 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/161 |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/162 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/163 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/164 |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/165 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/166 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/167 |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/168 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/169 |
| Improper Neutralization of Input During Web Page | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/170 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/171 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/172 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/173 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/174 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/175 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/176 |
| Insertion of Sensitive Informatio | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/177 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n into Log File | | | installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/178 |
| Improper Limitation of a Pathname to a Restricted Directory | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/179 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Path Traversal') | | | versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/180 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/181 |
| **Product: big-ip_application_acceleration_manager** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/182 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/183 |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/184 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/185 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/186 |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/187 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/188 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/189 |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/190 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/191 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/192 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/193 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/194 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/195 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/196 |
| Improper Neutralization of Input During Web Page Generation | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/197 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/198 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28708** | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/199 |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/200 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-29473** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/201 |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/202 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/203 |
| **Product: big-ip_application_security_manager** | | | | | |
| Missing Authentication for | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/204 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Critical Function | | | 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/205 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | | |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/206 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/207 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/208 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-26415** | | |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/209 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/210 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Always-Incorrect Control Flow Implementation | 05-May-22 | 7.5 | On F5 BIG-IP Advanced WAF, ASM, and APM 16.1.x versions prior to 16.1.2.1, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when ASM or Advanced WAF, as well as APM, are configured on a virtual server, the ASM policy is configured with Session Awareness, and the "Use APM Username and Session ID" option is enabled, undisclosed requests can cause the bd process to terminate. Note: | https://support.f5.com/csp/article/K03442392 | A-F5-BIG--200522/211 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26890** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/212 |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/213 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/214 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 7.2 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing command injection vulnerabilities in undisclosed URIs in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27806** | https://support.f5.com/csp/article/K68647001 | A-F5-BIG--200522/215 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/216 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/217 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/218 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/219 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/220 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/221 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/222 |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/223 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/224 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/225 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/226 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/227 |
| NULL Pointer Dereference | 05-May-22 | 7.5 | On F5 BIG-IP LTM, Advanced WAF, ASM, or APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a virtual server is configured with HTTP, TCP on one side (client/server), and DTLS on the other (server/client), undisclosed requests | https://support.f5.com/csp/article/K14229426 | A-F5-BIG--200522/228 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | can cause the TMM process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29491** | | |
| **Product: big-ip_carrier-grade_nat** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 8.8 | On 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x 11.6.x, a DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP AFM, CGNAT, and PEM Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28716** | https://support.f5.com/csp/article/K25451853 | A-F5-BIG--200522/229 |
| **Product: big-ip_domain_name_system** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/230 |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/231 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | | |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/232 |
| Uncontrolled Resource | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/233 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/234 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | | |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/235 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/236 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/237 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-27182** | | |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/238 |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/239 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/240 |
| Uncontrolled Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/241 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/242 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-28705** | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/243 |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/244 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/245 |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/246 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/247 |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/248 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/249 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/250 |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/251 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | | |
| **Product: big-ip_fraud_protection_service** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/252 |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/253 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | | |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/254 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/255 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/256 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | | |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/257 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/258 |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/259 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | | |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/260 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/261 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/262 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/263 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/264 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | | |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/265 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/266 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/267 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/268 |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/269 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/270 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/271 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/272 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/273 |
| **Product: big-ip_global_traffic_manager** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-1388** | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/274 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/275 |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/276 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/277 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/278 |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/279 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/280 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/281 |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/282 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/283 |
| Improper Neutralization of Input During Web Page Generation | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/284 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/285 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/286 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/287 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/288 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/289 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/290 |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/291 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/292 |
| Improper Limitation of a Pathname to a Restricted Directory | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/293 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Path Traversal') | | | 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/294 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/295 |
| **Product: big-ip_guided_configuration** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.1 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP APM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of F5 BIG-IP Guided | https://support.f5.com/csp/article/K21317311 | A-F5-BIG--200522/296 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Configuration that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27230** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 7.2 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing command injection vulnerabilities in undisclosed URIs in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27806** | https://support.f5.com/csp/article/K68647001 | A-F5-BIG--200522/297 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/298 |
| **Product: big-ip_link_controller** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/299 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/300 |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/301 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/302 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/303 |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/304 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/305 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/306 |
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/307 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/308 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/309 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/310 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/311 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/312 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/313 |
| Improper Neutralization of Input During Web Page Generation | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/314 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | | |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/315 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28708** | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/316 |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/317 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-29473** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/318 |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/319 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/320 |
| **Product: big-ip_local_traffic_manager** | | | | | |
| Missing Authentication for | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/321 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Critical Function | | | 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/322 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | | |
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26370** | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/323 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/324 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | DNS listener is configured on a virtual server with DNS queueing (default), undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/325 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-26415** | | |
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/326 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/327 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Shell (tmsh) commands in F5 BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/328 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Conversion between Numeric Types | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/329 |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/330 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management User Interface (TMUI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/331 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/332 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/333 |
| Integer Overflow or | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/334 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Wraparound | | | 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/335 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28706** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/336 |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/337 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | | |
| Insertion of Sensitive Information into Log File | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/338 |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/339 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/340 |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/341 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/342 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-29480** | | |
| NULL Pointer Dereference | 05-May-22 | 7.5 | On F5 BIG-IP LTM, Advanced WAF, ASM, or APM 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a virtual server is configured with HTTP, TCP on one side (client/server), and DTLS on the other (server/client), undisclosed requests can cause the TMM process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29491** | https://support.f5.com/csp/article/K14229426 | A-F5-BIG--200522/343 |
| **Product: big-ip_policy_enforcement_manager** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 9.8 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests | https://support.f5.com/csp/article/K23605346 | A-F5-BIG--200522/344 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-1388** | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/345 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Uninitialized Resource | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, and 14.1.x versions prior to 14.1.4.6, when a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2022-26370** | https://support.f5.com/csp/article/K51539421 | A-F5-BIG--200522/346 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.0.2, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when a DNS listener is configured on a virtual server with DNS queueing (default), | https://support.f5.com/csp/article/K23454411 | A-F5-BIG--200522/347 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.<br>**CVE ID : CVE-2022-26372** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.1 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26415** | https://support.f5.com/csp/article/K81952114 | A-F5-BIG--200522/348 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Incorrect Calculation | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when the BIG-IP CGNAT Large Scale NAT (LSN) pool is configured on a virtual server and packet filtering is enabled, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26517** | https://support.f5.com/csp/article/K54082580 | A-F5-BIG--200522/349 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, directory traversal vulnerabilities exist in undisclosed iControl REST endpoints and TMOS Shell (tmsh) commands in F5 | https://support.f5.com/csp/article/K53197140 | A-F5-BIG--200522/350 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | BIG-IP Guided Configuration, which may allow an authenticated attacker with at least resource administrator role privileges to read arbitrary files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26835** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, when BIG-IP packet filters are enabled and a virtual server is configured with the type set to Reject, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27182** | https://support.f5.com/csp/article/K31856317 | A-F5-BIG--200522/351 |
| Incorrect Conversion between | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to | https://support.f5.com/csp/article/K16187341 | A-F5-BIG--200522/352 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Numeric Types | | | 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when an Internet Content Adaptation Protocol (ICAP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27189** | | |
| Improper Privilege Management | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, an authenticated attacker can modify or delete Dashboards created by other BIG-IP users in the Traffic Management User Interface (TMUI). Note: Software versions which have | https://support.f5.com/csp/article/K41877405 | A-F5-BIG--200522/353 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27659** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 6.8 | On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27878** | https://support.f5.com/csp/article/K92807525 | A-F5-BIG--200522/354 |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when a Real Time Streaming | https://support.f5.com/csp/article/K37155600 | A-F5-BIG--200522/355 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Protocol (RTSP) profile is configured on a virtual server, undisclosed traffic can cause an increase in Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28691** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28701** | https://support.f5.com/csp/article/K99123750 | A-F5-BIG--200522/356 |
| Integer Overflow or Wraparound | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to | https://support.f5.com/csp/article/K52340447 | A-F5-BIG--200522/357 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 13.1.5, on platforms with an ePVA and the pva.fwdaccel BigDB variable enabled, undisclosed requests to a virtual server with a FastL4 profile that has ePVA acceleration enabled can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28705** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 16.1.x versions prior to 16.1.2 and 15.1.x versions prior to 15.1.5.1, when the DNS resolver configuration is used, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28706** | https://support.f5.com/csp/article/K03755971 | A-F5-BIG--200522/358 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, and 14.1.x versions prior to 14.1.4.6, a stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility (also referred to as the BIG-IP TMUI) that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28707** | https://support.f5.com/csp/article/K70300233 | A-F5-BIG--200522/359 |
| Improper Input Validation | 05-May-22 | 5.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2 and 15.1.x versions prior to 15.1.5.1, when a BIG-IP DNS resolver-enabled, HTTP-Explicit or SOCKS profile is configured on a virtual server, an undisclosed DNS response can cause the Traffic Management Microkernel (TMM) | https://support.f5.com/csp/article/K85054496 | A-F5-BIG--200522/360 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28708** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 8.8 | On 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x 11.6.x, a DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP AFM, CGNAT, and PEM Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28716** | https://support.f5.com/csp/article/K25451853 | A-F5-BIG--200522/361 |
| Insertion of Sensitive Informatio | 05-May-22 | 6.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1 and 14.1.x versions prior to | https://support.f5.com/csp/article/K47662005 | A-F5-BIG--200522/362 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n into Log File | | | 14.1.4.6, when installing Net HSM, the scripts (nethsm-safenet-install.sh and nethsm-thales-install.sh) expose the Net HSM partition password. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-28859** | | |
| Improper Check for Unusual or Exceptional Conditions | 05-May-22 | 7.5 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, and 13.1.x versions prior to 13.1.5, when an IPSec ALG profile is configured on a virtual server, undisclosed responses can cause Traffic Management Microkernel(TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29473** | https://support.f5.com/csp/article/K06323049 | A-F5-BIG--200522/363 |
| Improper Limitation of a Pathname to a Restricted | 05-May-22 | 4.3 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to | https://support.f5.com/csp/article/K59904248 | A-F5-BIG--200522/364 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, a directory traversal vulnerability exists in iControl SOAP that allows an authenticated attacker with at least guest role privileges to read wsdl files in the BIG-IP file system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29474** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/365 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | decreased performance. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| Uncontrolled Resource Consumption | 05-May-22 | 5.3 | On F5 BIG-IP 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, when multiple route domains are configured, undisclosed requests to big3d can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29480** | https://support.f5.com/csp/article/K71103363 | A-F5-BIG--200522/366 |
| **Product: big-iq_centralized_management** | | | | | |
| Incorrect Permission Assignment for Critical Resource | 05-May-22 | 4.9 | On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized | https://support.f5.com/csp/article/K38271531 | A-F5-BIG--200522/367 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management all versions of 8.x and 7.x, an authenticated, high-privileged attacker with no bash access may be able to access Certificate and Key files using Secure Copy (SCP) protocol from a remote system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-26340** | | |
| Improper Input Validation | 05-May-22 | 5.3 | On F5 BIG-IP 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x and 11.6.x, and F5 BIG-IQ Centralized Management all versions of 8.x and 7.x, when an IPv6 self IP address is configured and the ipv6.strictcompliance database key is enabled (disabled by default) on a BIG-IP system, undisclosed packets may cause decreased performance. Note: Software versions | https://support.f5.com/csp/article/K64124988 | A-F5-BIG--200522/368 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-29479** | | |
| **Product: nginx_service_mesh** | | | | | |
| Missing Authentication for Critical Function | 05-May-22 | 6.5 | On all versions 1.3.x (fixed in 1.4.0) NGINX Service Mesh control plane endpoints are exposed to the cluster overlay network. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27495** | https://support.f5.com/csp/article/K94093538 | A-F5-NGIN-200522/369 |
| **Product: traffix_signaling_delivery_controller** | | | | | |
| N/A | 05-May-22 | 4.8 | On F5 Traffix SDC 5.2.x versions prior to 5.2.2 and 5.1.x versions prior to 5.1.35, a stored Cross-Site Template Injection vulnerability exists in an undisclosed page of the Traffix SDC Configuration utility that allows an attacker to execute template language-specific instructions in the context of the server. Note: Software versions which have reached | https://support.f5.com/csp/article/K24248011 | A-F5-TRAF-200522/370 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27662** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 4.8 | On F5 Traffix SDC 5.2.x versions prior to 5.2.2 and 5.1.x versions prior to 5.1.35, a stored Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the Traffix SDC Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated<br>**CVE ID : CVE-2022-27880** | https://support.f5.com/csp/article/K17341495 | A-F5-TRAF-200522/371 |
| **Vendor: facturascripts** | | | | | |
| **Product: facturascripts** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site scripting - Reflected in Create Subaccount in GitHub repository neorazorx/facturascripts prior to 2022.07. This vulnerability can be arbitrarily executed javascript code to steal user'cookie, | https://huntr.dev/bounties/4578a690-73e5-4313-840c-ee15e5329741, https://github.com/neorazorx/facturascripts/commit/482c5a82b4d79e7a196 | A-FAC-FACT-200522/372 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | perform HTTP request, get content of `same origin` page, etc ...<br>**CVE ID : CVE-2022-1571** | 14f5a67dc24593046cefd | |
| **Vendor: fantastic_blog_project** | | | | | |
| **Product: fantastic_blog** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 04-May-22 | 9.8 | A SQL injection vulnerability exists in Sourcecodester Fantastic Blog CMS 1.0 . An attacker can inject query in "/fantasticblog/single.php" via the "id=5" parameters.<br>**CVE ID : CVE-2022-28512** | N/A | A-FAN-FANT-200522/373 |
| **Vendor: fastflow** | | | | | |
| **Product: fastflow** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 6.1 | The Fast Flow WordPress plugin before 1.2.11 does not sanitise and escape the page parameter before outputting back in an attribute in an admin dashboard, leading to a Reflected Cross-Site Scripting<br>**CVE ID : CVE-2022-1269** | N/A | A-FAS-FAST-200522/374 |
| **Vendor: ffjpeg_project** | | | | | |
| **Product: ffjpeg** | | | | | |
| Integer Overflow or | 05-May-22 | 6.5 | In ffjpeg (commit hash: caade60), the function bmp_load() in bmp.c contains an | N/A | A-FFJ-FFJP-200522/375 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Wraparound | | | integer overflow vulnerability, which eventually results in the heap overflow in jfif_encode() in jfif.c. This is due to the incomplete patch for issue 38<br>**CVE ID : CVE-2022-28471** | | |
| **Vendor: Ffmpeg** | | | | | |
| **Product: ffmpeg** | | | | | |
| Integer Overflow or Wraparound | 02-May-22 | 5.5 | An integer overflow vulnerability was found in FFmpeg 5.0.1 and in previous versions in g729_parse() in llibavcodec/g729_parser.c when processing a specially crafted file.<br>**CVE ID : CVE-2022-1475** | https://trac.ffmpeg.org/ticket/9651, https://bugzilla.redhat.com/show_bug.cgi?id=2076764 | A-FFM-FFMP-200522/376 |
| **Vendor: fluxcd** | | | | | |
| **Product: flux2** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 06-May-22 | 8.8 | Flux is an open and extensible continuous delivery solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to expose sensitive data from the controllerâ€™s pod filesystem and possibly privilege | https://github.com/fluxcd/flux2/security/advisories/GHSA-j77r-2fxf-5jrw | A-FLU-FLUX-200522/377 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation in multi-tenancy deployments. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 v0.29.0.<br>**CVE ID : CVE-2022-24877** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 06-May-22 | 6.5 | Flux is an open and extensible continuous delivery solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to cause a Denial of Service at the controller level. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 | https://github.com/fluxcd/flux2/security/advisories/GHSA-7pwf-jg34-hxwp | A-FLU-FLUX-200522/378 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | v0.29.0. Users are recommended to upgrade.<br>**CVE ID : CVE-2022-24878** | | |
| **Product: kustomize-controller** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 06-May-22 | 8.8 | Flux is an open and extensible continuous delivery solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to expose sensitive data from the controllerâ€™s pod filesystem and possibly privilege escalation in multi-tenancy deployments. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 v0.29.0.<br>**CVE ID : CVE-2022-24877** | https://github.com/fluxcd/flux2/security/advisories/GHSA-j77r-2fxf-5jrw | A-FLU-KUST-200522/379 |
| Improper Limitation of a | 06-May-22 | 6.5 | Flux is an open and extensible continuous delivery | https://github.com/fluxcd/flux2/security/advi | A-FLU-KUST-200522/380 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pathname to a Restricted Directory ('Path Traversal') | | | solution for Kubernetes. Path Traversal in the kustomize-controller via a malicious `kustomization.yaml` allows an attacker to cause a Denial of Service at the controller level. Workarounds include automated tooling in the user's CI/CD pipeline to validate `kustomization.yaml` files conform with specific policies. This vulnerability is fixed in kustomize-controller v0.24.0 and included in flux2 v0.29.0. Users are recommended to upgrade.<br>**CVE ID : CVE-2022-24878** | sories/GHSA-7pwf-jg34-hxwp | |
| **Vendor: Fortinet** | | | | | |
| **Product: fortisoar** | | | | | |
| Incorrect Authorization | 04-May-22 | 7.5 | An improper access control in Fortinet FortiSOAR before 7.2.0 allows unauthenticated attackers to access gateway API data via crafted HTTP GET requests.<br>**CVE ID : CVE-2022-23443** | https://fortiguard.com/psirt/FG-IR-22-041 | A-FOR-FORT-200522/381 |
| **Vendor: Foxit** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: pdf_reader** | | | | | |
| NULL Pointer Dereference | 05-May-22 | 5.5 | Foxit PDF Reader v11.2.1.53537 was discovered to contain a NULL pointer dereference via the component FoxitPDFReader.exe. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PHP file. **CVE ID : CVE-2022-27359** | N/A | A-FOX-PDF_-200522/382 |
| **Vendor: Freedesktop** | | | | | |
| **Product: poppler** | | | | | |
| N/A | 05-May-22 | 6.5 | A logic error in the Hints::Hints function of Poppler v22.03.0 allows attackers to cause a Denial of Service (DoS) via a crafted PDF file. **CVE ID : CVE-2022-27337** | https://gitlab.freedesktop.org/poppler/poppler/-/issues/1230, https://gitlab.freedesktop.org/poppler/poppler/-/issues/1230#note_1372177 | A-FRE-POPP-200522/383 |
| **Vendor: fusionpbx** | | | | | |
| **Product: fusionpbx** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 9.8 | Fusionpbx v4.4 and below contains a command injection vulnerability via the download email logs function. **CVE ID : CVE-2022-28055** | https://github.com/fusionpbx/fusionpbx/commit/4e260b170e17705c4c9ccf787be7711b63a40868 | A-FUS-FUSI-200522/384 |
| **Vendor: ghost** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: sqlite3** | | | | | |
| N/A | 01-May-22 | 7.5 | The package sqlite3 before 5.0.3 are vulnerable to Denial of Service (DoS) which will invoke the toString function of the passed parameter. If passed an invalid Function object it will throw and crash the V8 engine.<br>**CVE ID : CVE-2022-21227** | https://github.com/TryGhost/node-sqlite3/commit/593c9d498be2510d286349134537e3bf89401c4a | A-GHO-SQLI-200522/385 |
| **Vendor: git-pull-or-clone_project** | | | | | |
| **Product: git-pull-or-clone** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 01-May-22 | 9.8 | The package git-pull-or-clone before 2.0.2 are vulnerable to Command Injection due to the use of the --upload-pack feature of git which is also supported for git clone. The source includes the use of the secure child process API spawn(). However, the outpath parameter passed to it may be a command-line argument to the git clone command and result in arbitrary command injection.<br>**CVE ID : CVE-2022-24437** | https://github.com/feross/git-pull-or-clone/commit/f9ce092be13cc32e685dfa26e7705e9c6e3108a3 | A-GIT-GIT--200522/386 |
| **Vendor: gitea** | | | | | |
| **Product: gitea** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 7.5 | An arbitrary file deletion vulnerability in Gitea v1.16.3 allows attackers to cause a Denial of Service (DoS) via deleting the configuration file. **CVE ID : CVE-2022-27313** | https://github.com/go-gitea/gitea/pull/19072 | A-GIT-GITE-200522/387 |
| **Vendor: gogs** | | | | | |
| **Product: gogs** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | Stored xss bug in GitHub repository gogs/gogs prior to 0.12.7. As the repo is public , any user can view the report and when open the attachment then xss is executed. This bug allow executed any javascript code in victim account . **CVE ID : CVE-2022-1464** | https://github.com/gogs/gogs/commit/bc77440b301ac8780698be91dff1ac33b7cee850, https://huntr.dev/bounties/34a12146-3a5d-4efc-a0f8-7a3ae04b198d | A-GOG-GOGS-200522/388 |
| **Vendor: Google** | | | | | |
| **Product: gson** | | | | | |
| Deserialization of Untrusted Data | 01-May-22 | 7.5 | The package com.google.code.gson:gson before 2.8.9 are vulnerable to Deserialization of Untrusted Data via the writeReplace() method in internal classes, which may lead to DoS attacks. **CVE ID : CVE-2022-25647** | https://github.com/google/gson/pull/1991, https://github.com/google/gson/pull/1991/commits | A-GOO-GSON-200522/389 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: gpac** | | | | | |
| **Product: gpac** | | | | | |
| Reachable Assertion | 05-May-22 | 7.5 | In GPAC 2.1-DEV-rev87-g053aae8-master, function BS_ReadByte() in utils/bitstream.c has a failed assertion, which causes a Denial of Service. This vulnerability was fixed in commit 9ea93a2.<br>**CVE ID : CVE-2022-29339** | https://github.com/gpac/gpac/commit/9ea93a2ec8f555ceed1ee27294cf94822f14f10f | A-GPA-GPAC-200522/390 |
| NULL Pointer Dereference | 05-May-22 | 7.5 | GPAC 2.1-DEV-rev87-g053aae8-master. has a Null Pointer Dereference vulnerability in gf_isom_parse_movie_boxes_internal due to improper return value handling of GF_SKIP_BOX, which causes a Denial of Service. This vulnerability was fixed in commit 37592ad.<br>**CVE ID : CVE-2022-29340** | https://github.com/gpac/gpac/commit/37592ad86c6ca934d34740012213e467acc4a3b0 | A-GPA-GPAC-200522/391 |
| **Vendor: hospital_management_system_project** | | | | | |
| **Product: hospital_management_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL | 03-May-22 | 9.8 | Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the adminname | N/A | A-HOS-HOSP-200522/392 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('SQL Injection') | | | parameter in admin.php.<br>**CVE ID : CVE-2022-27413** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 04-May-22 | 9.8 | Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the patient_contact parameter in patientsearch.php.<br>**CVE ID : CVE-2022-27420** | N/A | A-HOS-HOSP-200522/393 |
| **Vendor: hubspot** | | | | | |
| **Product: hubspot** | | | | | |
| Server-Side Request Forgery (SSRF) | 02-May-22 | 8.8 | The HubSpot WordPress plugin before 8.8.15 does not validate the proxy URL given to the proxy REST endpoint, which could allow users with the edit_posts capability (by default contributor and above) to perform SSRF attacks<br>**CVE ID : CVE-2022-1239** | N/A | A-HUB-HUBS-200522/394 |
| **Vendor: IBM** | | | | | |
| **Product: robotic_process_automation** | | | | | |
| N/A | 05-May-22 | 6.5 | A vulnerability exists where an IBM Robotic Process Automation 21.0.1 regular user is able to obtain view-only access to some | https://www.ibm.com/support/pages/node/6570235, https://exchange.xforce.ibmclou | A-IBM-ROBO-200522/395 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | admin pages in the Control Center IBM X-Force ID: 223029.<br>**CVE ID : CVE-2022-22415** | d.com/vulnerabilities/223029 | |
| N/A | 05-May-22 | 4.6 | IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with physical access to create an API request modified to create additional objects. IBM X-Force ID: 224159.<br>**CVE ID : CVE-2022-22434** | https://exchange.xforce.ibmcloud.com/vulnerabilities/224159, https://www.ibm.com/support/pages/node/6579959 | A-IBM-ROBO-200522/396 |
| **Product: robotic_process_automation_as_a_service** | | | | | |
| N/A | 05-May-22 | 4.6 | IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with physical access to create an API request modified to create additional objects. IBM X-Force ID: 224159.<br>**CVE ID : CVE-2022-22434** | https://exchange.xforce.ibmcloud.com/vulnerabilities/224159, https://www.ibm.com/support/pages/node/6579959 | A-IBM-ROBO-200522/397 |
| **Product: spectrum_scale** | | | | | |
| Inadequate Encryption Strength | 03-May-22 | 7.5 | IBM Spectrum Scale 5.1.0 through 5.1.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive | https://exchange.xforce.ibmcloud.com/vulnerabilities/221012, https://www.ibm.com/support/pages/node/6579139 | A-IBM-SPEC-200522/398 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information. IBM X-Force ID: 221012.<br>**CVE ID : CVE-2022-22368** | | |
| **Vendor: idqk** | | | | | |
| **Product: masuit.tools** | | | | | |
| N/A | 01-May-22 | 9.8 | All versions of package masuit.tools.core are vulnerable to Arbitrary Code Execution via the ReceiveVarData<T> function in the SocketClient.cs component. The socket client in the package can pass in the payload via the user-controllable input after it has been established, because this socket client transmission does not have the appropriate restrictions or type bindings for the BinaryFormatter.<br>**CVE ID : CVE-2022-21167** | N/A | A-IDQ-MASU-200522/399 |
| **Vendor: importwp** | | | | | |
| **Product: import_wp** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 02-May-22 | 7.2 | The Import WP WordPress plugin before 2.4.6 does not validate the imported file in some cases, allowing high privilege users such as admin to | N/A | A-IMP-IMPO-200522/400 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | upload arbitrary files (such as PHP), leading to RCE<br>**CVE ID : CVE-2022-1273** | | |
| **Vendor: jailed_project** | | | | | |
| **Product: jailed** | | | | | |
| N/A | 01-May-22 | 9.8 | All versions of package jailed are vulnerable to Sandbox Bypass via an exported alert() method which can access the main application. Exported methods are stored in the application.remote object.<br>**CVE ID : CVE-2022-23923** | N/A | A-JAI-JAIL-200522/401 |
| **Vendor: jflyfox** | | | | | |
| **Product: jfinal_cms** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-May-22 | 7.2 | Jfinal_cms 5.1.0 is vulnerable to SQL Injection via com.jflyfox.system.log.LogController.java.<br>**CVE ID : CVE-2022-28505** | N/A | A-JFL-JFIN-200522/402 |
| **Vendor: jquery_json-viewer_project** | | | | | |
| **Product: jquery_json-viewer** | | | | | |
| Improper Neutralization of Input During | 04-May-22 | 6.1 | The jquery.json-viewer library through 1.4.0 for Node.js does not properly escape | https://github.com/abodelot/jquery.json-viewer/pull/26 | A-JQU-JQUE-200522/403 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | characters such as < in a JSON object, as demonstrated by a SCRIPT element.<br>**CVE ID : CVE-2022-30241** | | |
| **Vendor: jsgui-lang-essentials_project** | | | | | |
| **Product: jsgui-lang-essentials** | | | | | |
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 01-May-22 | 9.8 | All versions of package jsgui-lang-essentials are vulnerable to Prototype Pollution due to allowing all Object attributes to be altered, including their magical attributes such as proto, constructor and prototype.<br>**CVE ID : CVE-2022-25301** | N/A | A-JSG-JSGU-200522/404 |
| **Vendor: keywordrush** | | | | | |
| **Product: content_egg** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 6.1 | The Content Egg WordPress plugin before 5.3.0 does not sanitise and escape the page parameter before outputting back in an attribute in the Autoblogging admin dashboard, leading to a Reflected Cross-Site Scripting<br>**CVE ID : CVE-2022-0428** | N/A | A-KEY-CONT-200522/405 |
| **Vendor: Libarchive** | | | | | |
| **Product: libarchive** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 04-May-22 | 5.5 | Libarchive v3.6.0 was discovered to contain a read memory access vulnerability via the function lzma_decode.<br>**CVE ID : CVE-2022-28066** | N/A | A-LIB-LIBA-200522/406 |
| **Vendor: librehealth** | | | | | |
| **Product: librehealth_ehr** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-May-22 | 8.8 | In LibreHealth EHR 2.0.0, lack of sanitization of the GET parameter payment_id in interface\billing\new_payment.php via interface\billing\payment_master.inc.php leads to SQL injection.<br>**CVE ID : CVE-2022-29938** | N/A | A-LIB-LIBR-200522/407 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-May-22 | 5.4 | In LibreHealth EHR 2.0.0, lack of sanitization of the GET parameters debug and InsId in interface\billing\sl_eob_process.php leads to multiple cross-site scripting (XSS) vulnerabilities.<br>**CVE ID : CVE-2022-29939** | N/A | A-LIB-LIBR-200522/408 |
| Improper Neutralization of Input During | 05-May-22 | 5.4 | In LibreHealth EHR 2.0.0, lack of sanitization of the GET parameters formseq and formid | N/A | A-LIB-LIBR-200522/409 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | in interface\orders\find_order_popup.php leads to multiple cross-site scripting (XSS) vulnerabilities.<br>**CVE ID : CVE-2022-29940** | | |
| **Vendor: libsdl** | | | | | |
| **Product: sdl_ttf** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.8 | SDL_ttf v2.0.18 and below was discovered to contain an arbitrary memory write via the function TTF_RenderText_Solid(). This vulnerability is triggered via a crafted TTF file.<br>**CVE ID : CVE-2022-27470** | https://github.com/libsdl-org/SDL_ttf/commit/db1b41ab8bde6723c24b866e466cad78c2fa0448, https://github.com/libsdl-org/SDL_ttf/issues/187 | A-LIB-SDL_-200522/410 |
| **Vendor: libwav_project** | | | | | |
| **Product: libwav** | | | | | |
| Use of Uninitialized Resource | 04-May-22 | 7.5 | The function wav_format_write in libwav.c in libwav through 2017-04-20 has an Use of Uninitialized Variable vulnerability.<br>**CVE ID : CVE-2022-28488** | https://github.com/marc-q/libwav/issues/29 | A-LIB-LIBW-200522/411 |
| **Vendor: libxmljs_project** | | | | | |
| **Product: libxmljs** | | | | | |
| Uncontrolled Resource | 01-May-22 | 7.5 | This affects all versions of package libxmljs. When | https://github.com/libxmljs/libxmljs/commit/ | A-LIB-LIBX-200522/412 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | invoking the libxmljs.parseXml function with a non-buffer argument the V8 code will attempt invoking the .toString method of the argument. If the argument's toString value is not a Function object V8 will crash.<br>**CVE ID : CVE-2022-21144** | 2501807bde9b38cfaed06d1e140487516d91379d, https://github.com/libxmljs/libxmljs/pull/594 | |
| **Vendor: lifterlms** | | | | | |
| **Product: lifterlms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 6.1 | The LifterLMS PayPal WordPress plugin before 1.4.0 does not sanitise and escape some parameters from the payment confirmation page before outputting them back in the page, leading to a Reflected Cross-Site Scripting issue<br>**CVE ID : CVE-2022-1250** | https://make.lifterlms.com/2022/04/04/lifterlms-paypal-version-1-4-0/ | A-LIF-LIFT-200522/413 |
| **Vendor: Linux** | | | | | |
| **Product: linux_kernel** | | | | | |
| Missing Initialization of Resource | 02-May-22 | 7.8 | An issue was discovered in the Linux kernel through 5.17.5. io_rw_init_file in fs/io_uring.c lacks initialization of kiocb->private. | https://github.com/torvalds/linux/commit/32452a3eb8b64e01e2be717f518c0be046975b9d | A-LIN-LINU-200522/414 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-29968** | | |
| **Vendor: Logitech** | | | | | |
| **Product: options** | | | | | |
| Cross-Site Request Forgery (CSRF) | 03-May-22 | 8.8 | An issue was discovered in Logitech Options. The OAuth 2.0 state parameter was not properly validated. This leaves applications vulnerable to CSRF attacks during authentication and authorization operations. **CVE ID : CVE-2022-0916** | https://support.logi.com/hc/en-us/articles/360025297893 | A-LOG-OPTI-200522/415 |
| **Vendor: luya** | | | | | |
| **Product: yii-helpers** | | | | | |
| Improper Neutralization of Formula Elements in a CSV File | 01-May-22 | 7.8 | Formula Injection/CSV Injection due to Improper Neutralization of Formula Elements in CSV File in GitHub repository luyadev/yii-helpers prior to 1.2.1. Successful exploitation can lead to impacts such as client-sided command injection, code execution, or remote ex-filtration of contained confidential data. | https://huntr.dev/bounties/fa6d6e75-bc7a-40f6-9bdd-2541318912d4, https://github.com/luyadev/yii-helpers/commit/9956ed63f516110c2b588471507b870e748c4cfb | A-LUY-YII--200522/416 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-1544** | | |
| **Vendor: Mantisbt** | | | | | |
| **Product: mantisbt** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | An XSS issue was discovered in browser_search_plugin.php in MantisBT before 2.25.2. Unescaped output of the return parameter allows an attacker to inject code into a hidden input field. **CVE ID : CVE-2022-28508** | https://mantisbt.org/ | A-MAN-MANT-200522/417 |
| **Vendor: marketingheroes** | | | | | |
| **Product: sitesupercharger** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | The SiteSuperCharger WordPress plugin before 5.2.0 does not validate, sanitise and escape various user inputs before using them in SQL statements via AJAX actions (available to both unauthenticated and authenticated users), leading to Unauthenticated SQL Injections **CVE ID : CVE-2022-0771** | N/A | A-MAR-SITE-200522/418 |
| **Vendor: materializecss** | | | | | |
| **Product: materialize** | | | | | |
| Improper Neutralizat | 01-May-22 | 5.4 | All versions of package materialize- | N/A | A-MAT-MATE-200522/419 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ion of Input During Web Page Generation ('Cross-site Scripting') | | | css are vulnerable to Cross-site Scripting (XSS) due to improper escape of user input (such as <not-a-tag />) that is being parsed as HTML/JavaScript, and inserted into the Document Object Model (DOM). This vulnerability can be exploited when the user-input is provided to the autocomplete component.<br>**CVE ID : CVE-2022-25349** | | |
| **Vendor: matio_project** | | | | | |
| **Product: matio** | | | | | |
| Missing Release of Memory after Effective Lifetime | 02-May-22 | 5.5 | A memory leak was discovered in matio 1.5.21 and earlier in Mat_VarReadNextInfo5() in mat5.c via a crafted file. This issue can potentially result in DoS.<br>**CVE ID : CVE-2022-1515** | https://bugzilla.redhat.com/show_bug.cgi?id=2079986 | A-MAT-MATI-200522/420 |
| **Vendor: mattermost** | | | | | |
| **Product: playbooks** | | | | | |
| Improper Privilege Management | 03-May-22 | 8.8 | Mattermost Playbooks plugin 1.25 and earlier fails to properly restrict user-level permissions, which allows playbook members to escalate | https://mattermost.com/security-updates/ | A-MAT-PLAY-200522/421 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | their membership privileges and perform actions restricted to playbook admins.<br>**CVE ID : CVE-2022-1548** | | |
| **Vendor: Mediawiki** | | | | | |
| **Product: rss_for_mediawiki** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 6.1 | The RSS extension before 2022-04-29 for MediaWiki allows XSS via an rss element (if the feed is in $wgRSSUrlWhitelist and $wgRSSAllowLinkTag is true).<br>**CVE ID : CVE-2022-29969** | https://gerrit.wikimedia.org/r/c/787807 | A-MED-RSS_-200522/422 |
| **Vendor: medical_hub_directory_site_project** | | | | | |
| **Product: medical_hub_directory_site** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-May-22 | 9.8 | Sourcecodester Medical Hub Directory Site 1.0 is vulnerable to SQL Injection via /mhds/clinic/view_details.php.<br>**CVE ID : CVE-2022-28533** | N/A | A-MED-MEDI-200522/423 |
| **Vendor: menlosecurity** | | | | | |
| **Product: email_isolation** | | | | | |
| N/A | 02-May-22 | 5.3 | Links may not be rewritten according to policy in some specially formatted emails. | https://www.menlosecurity.com/published-security-vulnerabilities/ | A-MEN-EMAI-200522/424 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-24974** | | |
| **Vendor: Microfocus** | | | | | |
| **Product: netiq_access_manager** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 6.1 | Reflected Cross Site Scripting (XSS) vulnerability in NetIQ Access Manager prior to 5.0.2 **CVE ID : CVE-2022-26325** | https://www.microfocus.com/documentation/access-manager/5.0/accessmanager502-release-notes/accessmanager502-release-notes.html#t4f2msu33v8h | A-MIC-NETI-200522/425 |
| URL Redirection to Untrusted Site ('Open Redirect') | 02-May-22 | 6.1 | Potential open redirection vulnerability when URL is crafted in specific format in NetIQ Access Manager prior to 5.0.2 **CVE ID : CVE-2022-26326** | https://www.microfocus.com/documentation/access-manager/5.0/accessmanager502-release-notes/accessmanager502-release-notes.html#t4f2msu33v8h | A-MIC-NETI-200522/426 |
| **Vendor: Microweber** | | | | | |
| **Product: microweber** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | DOM XSS in microweber ver 1.2.15 in GitHub repository microweber/microweber prior to 1.2.16. inject arbitrary js code, deface website, steal cookie... **CVE ID : CVE-2022-1555** | https://huntr.dev/bounties/d9f9b5bd-16f3-4eaa-9e36-d4958b557687, https://github.com/microweber/microweber/commit/724e2d186a33c0c2727 | A-MIC-MICR-200522/427 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 3107dc4f160a09384877f | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Reflected XSS in GitHub repository microweber/microweber prior to 1.2.16. Executing JavaScript as the victim **CVE ID : CVE-2022-1584** | https://github.com/microweber/microweber/commit/527abd148e6b7aff8df92a9f1aa951e5bebac59c, https://huntr.dev/bounties/69f4ca67-d615-4f25-b2d1-19df7bf1107d | A-MIC-MICR-200522/428 |
| **Vendor: mingsoft** | | | | | |
| **Product: mcms** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-May-22 | 9.8 | MCMS v5.2.27 was discovered to contain a SQL injection vulnerability in the orderBy parameter at /dict/list.do. **CVE ID : CVE-2022-27466** | N/A | A-MIN-MCMS-200522/429 |
| **Vendor: mingyuefusu_project** | | | | | |
| **Product: mingyuefusu** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-May-22 | 9.8 | mingyuefusu Library Management System all versions as of 03-27-2022 is vulnerable to SQL Injection. **CVE ID : CVE-2022-28461** | N/A | A-MIN-MING-200522/430 |
| **Vendor: Mozilla** | | | | | |
| **Product: convict** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 01-May-22 | 9.8 | The package convict before 6.2.2 are vulnerable to Prototype Pollution via the convict function due to missing validation of parentKey. **Note:** This vulnerability derives from an incomplete fix of another [vulnerability](https://security.snyk.io/vuln/SNYK-JS-CONVICT-1062508) **CVE ID : CVE-2022-22143** | https://snyk.io/vuln/SNYK-JS-CONVICT-2340604, https://github.com/mozilla/node-convict/commit/3b86be087d8f14681a9c889d45da7fe3ad9cd880 | A-MOZ-CONV-200522/431 |
| **Vendor: nanohttpd** | | | | | |
| **Product: nanohttpd** | | | | | |
| N/A | 01-May-22 | 5.5 | This affects all versions of package org.nanohttpd:nanohttpd. Whenever an HTTP Session is parsing the body of an HTTP request, the body of the request is written to a RandomAccessFile when the it is larger than 1024 bytes. This file is created with insecure permissions that allow its contents to be viewed by all users on the host machine. **Workaround:** Manually specifying the -Djava.io.tmpdir= argument when | N/A | A-NAN-NANO-200522/432 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | launching Java to set the temporary directory to a directory exclusively controlled by the current user can fix this issue.<br>**CVE ID : CVE-2022-21230** | | |
| **Vendor: nopcommerce** | | | | | |
| **Product: nopcommerce** | | | | | |
| URL Redirection to Untrusted Site ('Open Redirect') | 04-May-22 | 6.1 | In nopCommerce 4.50.1, an open redirect vulnerability can be triggered by luring a user to authenticate to a nopCommerce page by clicking on a crafted link.<br>**CVE ID : CVE-2022-27461** | http://nopcommerce.com | A-NOP-NOPC-200522/433 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 02-May-22 | 7.5 | nopCommerce 4.50.1 is vulnerable to Directory Traversal via the backup file in the Maintenance feature.<br>**CVE ID : CVE-2022-28451** | https://github.com/nopSolutions/nopCommerce/commit/47ff9a241243db9359f10216bcf401baaa36d0b4 | A-NOP-NOPC-200522/434 |
| **Vendor: novel-plus_project** | | | | | |
| **Product: novel-plus** | | | | | |
| Files or Directories Accessible to External Parties | 05-May-22 | 7.5 | novel-plus 3.6.0 suffers from an Arbitrary file reading vulnerability.<br>**CVE ID : CVE-2022-28462** | N/A | A-NOV-NOVE-200522/435 |
| **Vendor: octopus** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: server** | | | | | |
| Incorrect Authorization | 04-May-22 | 4.3 | Permissions were not properly verified in the API on projects using version control in Git. This allowed projects to be modified by users with only ProjectView permissions. **CVE ID : CVE-2022-1502** | https://advisories.octopus.com/post/2022/sa2022-03/ | A-OCT-SERV-200522/436 |
| **Vendor: ohler** | | | | | |
| **Product: agoo** | | | | | |
| N/A | 04-May-22 | 7.5 | ** DISPUTED ** Agoo before 2.14.3 does not reject GraphQL fragment spreads that form cycles, leading to an application crash. NOTE: the vendor has disputed this on the grounds that it is not the server's responsibility to "enforce all the various ways a developer could write code with logic errors." **CVE ID : CVE-2022-30288** | N/A | A-OHL-AGOO-200522/437 |
| **Vendor: Openldap** | | | | | |
| **Product: openldap** | | | | | |
| Improper Neutralization of Special | 04-May-22 | 9.8 | In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection | https://bugs.openldap.org/show_bug.cgi?id=9815 | A-OPE-OPEN-200522/438 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an SQL Command ('SQL Injection') | | | vulnerability exists in the experimental back-sql backend to slapd, via a SQL statement within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to a lack of proper escaping.<br>**CVE ID : CVE-2022-29155** | | |
| **Vendor: Openssl** | | | | | |
| **Product: openssl** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 03-May-22 | 9.8 | The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected | https://www.openssl.org/news/secadv/20220503.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1ad73b4d27bd8c1b369a3cd453681d3a4f1bb9b2, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=e5fd1728ef4c7a5bf7c7a7163ca60370460a6e23 | A-OPE-OPEN-200522/439 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).<br>**CVE ID : CVE-2022-1292** | | |
| Improper Certificate Validation | 03-May-22 | 5.3 | The function `OCSP_basic_verify` verifies the signer certificate on an OCSP response. In the case where the (non-default) flag OCSP_NOCHECKS is used then the response will be positive (meaning a successful verification) even in the case where the response signing certificate fails to verify. It is anticipated that most users of `OCSP_basic_verify` will not use the OCSP_NOCHECKS flag. In this case the `OCSP_basic_verify` function will return a negative value (indicating a fatal error) in the case of a certificate verification failure. The normal expected return value in this case would be 0. This issue also impacts | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2eda98790c5c2741d76d23cc1e74b0dc4f4b391a, https://www.openssl.org/news/secadv/20220503.txt | A-OPE-OPEN-200522/440 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the command line OpenSSL "ocsp" application. When verifying an ocsp response with the "-no_cert_checks" option the command line application will report that the verification is successful even though it has in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).<br>**CVE ID : CVE-2022-1343** | | |
| Use of a Broken or Risky Cryptographic Algorithm | 03-May-22 | 5.9 | The OpenSSL 3.0 implementation of the RC4-MD5 ciphersuite incorrectly uses the AAD data as the MAC key. This makes the MAC key trivially predictable. An attacker could exploit this issue by performing a man-in-the-middle attack to modify data being sent from one endpoint to an | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=7d56a74a96828985db7354a55227a511615f732b, https://www.openssl.org/news/secadv/20220503.txt | A-OPE-OPEN-200522/441 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | OpenSSL 3.0 recipient such that the modified data would still pass the MAC integrity check. Note that data sent from an OpenSSL 3.0 endpoint to a non-OpenSSL 3.0 endpoint will always be rejected by the recipient and the connection will fail at that point. Many application protocols require data to be sent from the client to the server first. Therefore, in such a case, only an OpenSSL 3.0 server would be impacted when talking to a non-OpenSSL 3.0 client. If both endpoints are OpenSSL 3.0 then the attacker could modify data being sent in both directions. In this case both clients and servers could be affected, regardless of the application protocol. Note that in the absence of an attacker this bug means that an OpenSSL 3.0 endpoint communicating with a non-OpenSSL 3.0 endpoint will fail to | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | complete the handshake when using this ciphersuite. The confidentiality of data is not impacted by this issue, i.e. an attacker cannot decrypt data that has been encrypted using this ciphersuite - they can only modify it. In order for this attack to work both endpoints must legitimately negotiate the RC4-MD5 ciphersuite. This ciphersuite is not compiled by default in OpenSSL 3.0, and is not available within the default provider or the default ciphersuite list. This ciphersuite will never be used if TLSv1.3 has been negotiated. In order for an OpenSSL 3.0 endpoint to use this ciphersuite the following must have occurred: 1) OpenSSL must have been compiled with the (non-default) compile time option enable-weak-ssl-ciphers 2) OpenSSL must have had the legacy provider | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | explicitly loaded (either through application code or via configuration) 3) The ciphersuite must have been explicitly added to the ciphersuite list 4) The libssl security level must have been set to 0 (default is 1) 5) A version of SSL/TLS below TLSv1.3 must have been negotiated 6) Both endpoints must negotiate the RC4-MD5 ciphersuite in preference to any others that both endpoints have in common Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).<br>**CVE ID : CVE-2022-1434** | | |
| Improper Resource Shutdown or Release | 03-May-22 | 7.5 | The OPENSSL_LH_flush() function, which empties a hash table, contains a bug that breaks reuse of the memory occuppied by the removed hash table entries. This function is used when decoding certificates or keys. If a long lived process periodically decodes certificates or keys its memory | https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=64c85430f95200b6b51fe9475bd5203f7c19daf1, https://www.openssl.org/news/secadv/20220503.txt | A-OPE-OPEN-200522/442 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | usage will expand without bounds and the process might be terminated by the operating system causing a denial of service. Also traversing the empty hash table entries will take increasingly more time. Typically such long lived processes might be TLS clients or TLS servers configured to accept client certificate authentication. The function was added in the OpenSSL 3.0 version thus older releases are not affected by the issue. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).<br>**CVE ID : CVE-2022-1473** | | |
| **Vendor: Opensuse** | | | | | |
| **Product: open_build_service** | | | | | |
| Improper Restriction of XML External Entity Reference | 03-May-22 | 8.8 | A Improper Restriction of XML External Entity Reference vulnerability in SUSE Open Build Service allows remote attackers to reference external entities in certain operations. This can be used to gain information from the | https://bugzilla.suse.com/show_bug.cgi?id=1197928 | A-OPE-OPEN-200522/443 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | server that can be abused to escalate to Admin privileges on OBS. This issue affects: SUSE Open Build Service Open Build Service versions prior to 2.10.13.<br>**CVE ID : CVE-2022-21949** | | |
| **Vendor: pagehelper_project** | | | | | |
| **Product: pagehelper** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 04-May-22 | 9.8 | MyBatis PageHelper v1.x.x-v5.x.x was discovered to contain a time-blind SQL injection vulnerability via the orderBy parameter.<br>**CVE ID : CVE-2022-28111** | N/A | A-PAG-PAGE-200522/444 |
| **Vendor: parseplatform** | | | | | |
| **Product: parse-server** | | | | | |
| Improper Certificate Validation | 04-May-22 | 7.5 | Improper validation of the Apple certificate URL in the Apple Game Center authentication adapter allows attackers to bypass authentication, making the server vulnerable to DoS attacks. The vulnerability has been fixed by improving the URL validation and adding additional checks of the | https://github.com/parse-community/parse-server/security/advisories/GHSA-qf8x-vqjv-92gr | A-PAR-PARS-200522/445 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | resource the URL points to before downloading it.<br>**CVE ID : CVE-2022-24901** | | |
| **Vendor: Phome** | | | | | |
| **Product: empirecms** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-May-22 | 9.8 | EmpireCMS 7.5 has a SQL injection vulnerability in AdClass.php<br>**CVE ID : CVE-2022-28585** | N/A | A-PHO-EMPI-200522/446 |
| **Vendor: Pingidentity** | | | | | |
| **Product: pingfederate** | | | | | |
| Improper Authentication | 02-May-22 | 6.5 | When a password reset mechanism is configured to use the Authentication API with an Authentication Policy, email One-Time Password, PingID or SMS authentication, an existing user can reset another existing userâ€™s password.<br>**CVE ID : CVE-2022-23722** | https://docs.pingidentity.com/bundle/pingfederate-110/page/spk1642790928508.html, https://www.pingidentity.com/en/resources/downloads/pingfederate.html | A-PIN-PING-200522/447 |
| **Product: pingone_mfa_integration_kit** | | | | | |
| Improper Authentication | 02-May-22 | 9.8 | An MFA bypass vulnerability exists in the PingFederate PingOne MFA Integration Kit when | https://docs.pingidentity.com/bundle/pingfederate-pingone-mfa- | A-PIN-PING-200522/448 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | adapter HTML templates are used as part of an authentication flow.<br>**CVE ID : CVE-2022-23723** | ik/page/wpt1599064234202.html, https://www.pingidentity.com/en/resources/downloads/pingfederate.html | |
| **Vendor: pistache_project** | | | | | |
| **Product: pistache** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 01-May-22 | 7.5 | This affects the package pistacheio/pistache before 0.0.3.20220425. It is possible to traverse directories to fetch arbitrary files from the server.<br>**CVE ID : CVE-2022-26068** | N/A | A-PIS-PIST-200522/449 |
| **Vendor: Pixelimity** | | | | | |
| **Product: Pixelimity** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 4.8 | A stored cross-site scripting (XSS) vulnerability in Pixelimity 1.0 allows attackers to execute arbitrary web scripts or HTML via the Title field in admin/pages.php?action=add_new<br>**CVE ID : CVE-2022-28589** | N/A | A-PIX-PIXE-200522/450 |
| N/A | 03-May-22 | 7.2 | A Remote Code Execution (RCE) vulnerability exists in Pixelimity 1.0 via admin/admin- | N/A | A-PIX-PIXE-200522/451 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ajax.php?action=install_theme.<br>**CVE ID : CVE-2022-28590** | | |
| **Vendor: poultry_farm_management_system_project** | | | | | |
| **Product: poultry_farm_management_system** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 04-May-22 | 8.8 | Poultry Farm Management System v1.0 was discovered to contain a SQL injection vulnerability via the Item parameter at /farm/store.php.<br>**CVE ID : CVE-2022-28099** | N/A | A-POU-POUL-200522/452 |
| **Vendor: Progress** | | | | | |
| **Product: openedge** | | | | | |
| Improper Privilege Management | 02-May-22 | 7.8 | In Progress OpenEdge before 11.7.14 and 12.x before 12.2.9, certain SUID binaries within the OpenEdge application were susceptible to privilege escalation. If exploited, a local attacker could elevate their privileges and compromise the affected system.<br>**CVE ID : CVE-2022-29849** | https://community.progress.com/s/article/OpenEdge-11-7-14-is-Now-Available, https://community.progress.com/s/article/OpenEdge-12-2-9-Update-is-available | A-PRO-OPEN-200522/453 |
| **Vendor: proxyscotch_project** | | | | | |
| **Product: proxyscotch** | | | | | |
| Server-Side Request | 01-May-22 | 7.5 | The package github.com/hoppscotch/proxyscotch | https://github.com/hoppscotch/proxyscotch/c | A-PRO-PROX-200522/454 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Forgery (SSRF) | | | before 1.0.0 are vulnerable to Server-side Request Forgery (SSRF) when interceptor mode is set to proxy. It occurs when an HTTP request is made by a backend server to an untrusted URL submitted by a user. It leads to a leakage of sensitive information from the server.<br>**CVE ID : CVE-2022-25850** | ommit/de67380f62f907f201d75854b76024ba4885fab7 | |
| **Vendor: python-libnmap_project** | | | | | |
| **Product: python-libnmap** | | | | | |
| Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | 04-May-22 | 9.8 | In the python-libnmap package through 0.7.2 for Python, remote command execution can occur (if used in a client application that does not validate arguments).<br>**CVE ID : CVE-2022-30284** | N/A | A-PYT-PYTH-200522/455 |
| **Vendor: Qnap** | | | | | |
| **Product: qvr** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Comman | 05-May-22 | 9.8 | We have already fixed this vulnerability in the following versions of QVR: QVR 5.1.6 build 20220401 and later<br>**CVE ID : CVE-2022-27588** | https://www.qnap.com/en/security-advisory/qsa-22-07 | A-QNA-QVR-200522/456 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| d Injection') | | | | | |
| **Vendor: rainier** | | | | | |
| **Product: open_virtual_simulation_experiment_teaching_management_platform** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 05-May-22 | 9.8 | Beijing Runnier Network Technology Co., Ltd Open virtual simulation experiment teaching management platform software 2.0 has a file upload vulnerability, which can be exploited by an attacker to gain control of the server. **CVE ID : CVE-2022-28120** | N/A | A-RAI-OPEN-200522/457 |
| **Vendor: Rainworx** | | | | | |
| **Product: auctionworx** | | | | | |
| Cross-Site Request Forgery (CSRF) | 02-May-22 | 8 | Rainworx Auctionworx < 3.1R2 is vulnerable to a Cross-Site Request Forgery (CSRF) attack that allows an authenticated user to upgrade his account to admin and gain access to the auctionworx admin control panel. This vulnerability affects AuctionWorx Enterprise and AuctionWorx: Events Edition. **CVE ID : CVE-2022-23904** | https://www.rainworx.com/ | A-RAI-AUCT-200522/458 |
| **Vendor: s-cart** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: s-cart** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-May-22 | 3.5 | The package s-cart/s-cart before 6.9; the package s-cart/core before 6.9 are vulnerable to Cross-site Scripting (XSS) which can lead to cookie stealing of any victim that visits the affected URL so the attacker can gain unauthorized access to that user's account through the stolen cookie.<br>**CVE ID : CVE-2022-21149** | N/A | A-S-C-S-CA-200522/459 |
| **Vendor: Samsung** | | | | | |
| **Product: galaxy_store** | | | | | |
| Improper Input Validation | 03-May-22 | 5.5 | Improper input validation vulnerability in InstallAgent in Galaxy Store prior to version 4.5.41.8 allows attacker to overwrite files stored in a specific path. The patch adds proper protection to prevent overwrite to existing files.<br>**CVE ID : CVE-2022-28791** | https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=5 | A-SAM-GALA-200522/460 |
| **Product: gear_iconx_pc_manager** | | | | | |
| Uncontrolled Search Path Element | 03-May-22 | 7.8 | DLL hijacking vulnerability in Gear IconX PC Manager prior to version 2.1.220405.51 | https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=5 | A-SAM-GEAR-200522/461 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allows attacker to execute arbitrary code. The patch adds proper absolute path to prevent dll hijacking.<br>**CVE ID : CVE-2022-28792** | | |
| **Product: link_to_windows_service** | | | | | |
| Improper Authentication | 03-May-22 | 3.3 | Improper authentication in Link to Windows Service prior to version 2.3.04.1 allows attacker to lock the device. The patch adds proper caller signature check logic.<br>**CVE ID : CVE-2022-28790** | https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=5 | A-SAM-LINK-200522/462 |
| **Product: voice_note** | | | | | |
| Missing Authorization | 03-May-22 | 5.5 | Unprotected activities in Voice Note prior to version 21.3.51.11 allows attackers to record voice without user interaction. The patch adds proper permission for vulnerable activities.<br>**CVE ID : CVE-2022-28789** | https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=5 | A-SAM-VOIC-200522/463 |
| **Vendor: sandboxie** | | | | | |
| **Product: sandboxie** | | | | | |
| Incorrect Authorization | 04-May-22 | 8.6 | An incorrect access control issue in Sandboxie Classic v5.55.13 allows attackers to cause a | N/A | A-SAN-SAND-200522/464 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Denial of Service (DoS) in the Sandbox via a crafted executable.<br>**CVE ID : CVE-2022-28067** | | |
| **Vendor: Schedmd** | | | | | |
| **Product: slurm** | | | | | |
| Improper Authentication | 05-May-22 | 8.8 | SchedMD Slurm 21.08.x through 20.11.x has Incorrect Access Control that leads to Information Disclosure.<br>**CVE ID : CVE-2022-29500** | https://lists.schedmd.com/pipermail/slurm-announce/, https://www.schedmd.com/news.php, https://www.schedmd.com/news.php?id=260 | A-SCH-SLUR-200522/465 |
| N/A | 05-May-22 | 8.8 | SchedMD Slurm 21.08.x through 20.11.x has Incorrect Access Control that leads to Escalation of Privileges and code execution.<br>**CVE ID : CVE-2022-29501** | https://lists.schedmd.com/pipermail/slurm-announce/, https://www.schedmd.com/news.php, https://www.schedmd.com/news.php?id=260 | A-SCH-SLUR-200522/466 |
| N/A | 05-May-22 | 9.8 | SchedMD Slurm 21.08.x through 20.11.x has Incorrect Access Control that leads to Escalation of Privileges.<br>**CVE ID : CVE-2022-29502** | https://lists.schedmd.com/pipermail/slurm-announce/, https://www.schedmd.com/news.php, https://www.schedmd.com/news.php?id=260 | A-SCH-SLUR-200522/467 |
| **Vendor: seacms** | | | | | |
| **Product: seacms** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 04-May-22 | 7.2 | Seacms v11.6 was discovered to contain a remote command execution (RCE) vulnerability via the Mail Server Settings.<br>**CVE ID : CVE-2022-28076** | N/A | A-SEA-SEAC-200522/468 |
| **Vendor: secomea** | | | | | |
| **Product: gatemanager** | | | | | |
| N/A | 04-May-22 | 4.9 | Unprotected Alternate Channel vulnerability in debug console of GateManager allows system administrator to obtain sensitive information. This issue affects: GateManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25786** | https://www.secomea.com/support/cybersecurity-advisory/ | A-SEC-GATE-200522/469 |
| **Vendor: Shopizer** | | | | | |
| **Product: shopizer** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-May-22 | 4.8 | A Stored Cross Site Scripting (XSS) vulnerability exists in Shopizer versions 2.0 through 2.17.0, where a privileged user (attacker) can inject malicious JavaScript in the filename under the “Manage files” tab<br>**CVE ID : CVE-2022-23060** | https://github.com/shopizer-ecommerce/shopizer/commit/6b9f1ecd303b3b724d96bd08095c1a751dcc287e | A-SHO-SHOP-200522/470 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Authorization Bypass Through User-Controlled Key | 01-May-22 | 6.5 | In Shopizer versions 2.0 to 2.17.0 a regular admin can permanently delete a superadmin (although this cannot happen according to the documentation) via Insecure Direct Object Reference (IDOR) vulnerability. **CVE ID : CVE-2022-23061** | https://github.com/shopizer-ecommerce/shopizer/commit/6b9f1ecd303b3b724d96bd08095c1a751dcc287e | A-SHO-SHOP-200522/471 |
| Insufficient Session Expiration | 03-May-22 | 8.8 | In Shopizer versions 2.3.0 to 3.0.1 are vulnerable to Insufficient Session Expiration. When a password has been changed by the user or by an administrator, a user that was already logged in, will still have access to the application even after the password was changed. **CVE ID : CVE-2022-23063** | N/A | A-SHO-SHOP-200522/472 |
| **Vendor: shopxo** | | | | | |
| **Product: shopxo** | | | | | |
| Incorrect Permission Assignment for Critical Resource | 02-May-22 | 9.8 | ShopXO v2.2.5 and below was discovered to contain a system re-install vulnerability via the Add function in app/install/controller/Index.php. | N/A | A-SHO-SHOP-200522/473 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28056** | | |
| **Vendor: simple_doctor\'s_appointment_system_project** | | | | | |
| **Product: simple_doctor\'s_appointment_system** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 04-May-22 | 9.8 | Sourcecodester Doctor's Appointment System 1.0 is vulnerable to File Upload to RCE via Image upload from the administrator panel. An attacker can obtain remote command execution just by knowing the path where the images are stored. **CVE ID : CVE-2022-28568** | N/A | A-SIM-SIMP-200522/474 |
| **Vendor: sinatrarb** | | | | | |
| **Product: sinatra** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 02-May-22 | 7.5 | Sinatra before 2.2.0 does not validate that the expanded path matches public_dir when serving static files. **CVE ID : CVE-2022-29970** | https://github.com/sinatra/sinatra/pull/1683/commits/462c3ca1db53ed3cfc394cf5948e9c948ad1c10e | A-SIN-SINA-200522/475 |
| **Vendor: sitemap_project** | | | | | |
| **Product: sitemap** | | | | | |
| Missing Authorization | 02-May-22 | 8.8 | The Sitemap by click5 WordPress plugin before 1.0.36 does not have authorisation and CSRF checks when updating options via | N/A | A-SIT-SITE-200522/476 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | a REST endpoint, and does not ensure that the option to be updated belongs to the plugin. As a result, unauthenticated attackers could change arbitrary blog options, such as the users_can_register and default_role, allowing them to create a new admin account and take over the blog.<br>**CVE ID : CVE-2022-0952** | | |
| **Vendor: skycaiji** | | | | | |
| **Product: skycaiji** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 04-May-22 | 7.2 | Skycaiji v2.4 was discovered to contain a remote code execution (RCE) vulnerability via /SkycaijiApp/admin/controller/Develop.php.<br>**CVE ID : CVE-2022-28096** | N/A | A-SKY-SKYC-200522/477 |
| **Vendor: snipeitapp** | | | | | |
| **Product: snipe-it** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a | 02-May-22 | 8.8 | In Snipe-IT, versions v3.0-alpha to v5.3.7 are vulnerable to Host Header Injection. By sending a specially crafted host header in the | https://github.com/snipe/snipe-it/commit/0c4768fd2a11ac26a61814cef23a71061bfd8bcc | A-SNI-SNIP-200522/478 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Downstream Component ('Injection') | | | reset password request, it is possible to send password reset links to users which once clicked lead to an attacker controlled server and thus leading to password reset token leak. This leads to account take over.<br>**CVE ID : CVE-2022-23064** | | |
| **Vendor: Splunk** | | | | | |
| **Product: splunk** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-May-22 | 6.1 | The Monitoring Console app configured in Distributed mode allows for a Reflected XSS in a query parameter in Splunk Enterprise versions before 8.1.4. The Monitoring Console app is a bundled app included in Splunk Enterprise, not for download on SplunkBase, and not installed on Splunk Cloud Platform instances. Note that the Cloud Monitoring Console is not impacted.<br>**CVE ID : CVE-2022-27183** | https://research.splunk.com/application/splunk_xss_in_monitoring_console/, https://www.splunk.com/en_us/product-security/announcements/svd-2022-0505.html | A-SPL-SPLU-200522/479 |
| **Vendor: springbootmovie_project** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: springbootmovie** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 5.4 | In SpringBootMovie <=1.2 when adding movie names, malicious code can be stored because there are no filtering parameters, resulting in stored XSS. **CVE ID : CVE-2022-28588** | N/A | A-SPR-SPRI-200522/480 |
| Unrestricted Upload of File with Dangerous Type | 03-May-22 | 7.2 | In SpringBootMovie <=1.2, the uploaded file suffix parameter is not filtered, resulting in arbitrary file upload vulnerability **CVE ID : CVE-2022-29001** | N/A | A-SPR-SPRI-200522/481 |
| **Vendor: squirrel-lang** | | | | | |
| **Product: squirrel** | | | | | |
| Out-of-bounds Write | 04-May-22 | 10 | thread_call in sqbaselib.cpp in SQUIRREL 3.2 lacks a certain sq_reservestack call. **CVE ID : CVE-2022-30292** | https://github.com/albertodemichelis/squirrel/commit/a6413aa690e0bdfef648c68693349a7b878fe60d | A-SQU-SQUI-200522/482 |
| **Vendor: sscms** | | | | | |
| **Product: siteserver_cms** | | | | | |
| N/A | 03-May-22 | 9.8 | SiteServer CMS v7.x allows attackers to execute arbitrary code via a crafted plug-in. **CVE ID : CVE-2022-28118** | N/A | A-SSC-SITE-200522/483 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Vendor: talend** | | | | | |
| **Product: administration_center** | | | | | |
| Server-Side Request Forgery (SSRF) | 04-May-22 | 6.5 | Talend Administration Center has a vulnerability that allows an authenticated user to use the Service Registry 'Add' functionality to perform SSRF HTTP GET requests on URLs in the internal network. The issue is fixed for versions 8.0.x in TPS-5189, versions 7.3.x in TPS-5175, and versions 7.2.x in TPS-5201. Earlier versions of Talend Administration Center may also be impacted; users are encouraged to update to a supported version.<br>**CVE ID : CVE-2022-29942** | https://www.talend.com/security/incident-response/#CVE-2022-29942, https://Talend.com | A-TAL-ADMI-200522/484 |
| Improper Restriction of XML External Entity Reference | 04-May-22 | 6.5 | Talend Administration Center has a vulnerability that allows an authenticated user to use XML External Entity (XXE) processing to achieve read access as root on the remote filesystem. The issue is fixed for | https://www.talend.com/security/incident-response/#CVE-2022-29942, https://Talend.com | A-TAL-ADMI-200522/485 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions 8.0.x in TPS-5189, versions 7.3.x in TPS-5175, and versions 7.2.x in TPS-5201. Earlier versions of Talend Administration Center may also be impacted; users are encouraged to update to a supported version.<br>**CVE ID : CVE-2022-29943** | | |
| **Vendor: thedaylightstudio** | | | | | |
| **Product: fuel_cms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-May-22 | 5.4 | A stored cross-site scripting (XSS) vulnerability exists in FUEL-CMS 1.5.1 that allows an authenticated user to upload a malicious .pdf file which acts as a stored XSS payload. If this stored XSS payload is triggered by an administrator it will trigger a XSS attack.<br>**CVE ID : CVE-2022-28599** | N/A | A-THE-FUEL-200522/486 |
| **Vendor: trumpf** | | | | | |
| **Product: trutops_boost** | | | | | |
| Missing Authentication for Critical Function | 02-May-22 | 9.8 | Multiple Version of TRUMPF TruTops products expose a service function without necessary authentication. Execution of this | https://cert.vde.com/en/advisories/VDE-2022-016/ | A-TRU-TRUT-200522/487 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | function may result in unauthorized access to change of data or disruption of the whole service.<br>**CVE ID : CVE-2022-1300** | | |
| **Product: trutops_fab** | | | | | |
| Missing Authentication for Critical Function | 02-May-22 | 9.8 | Multiple Version of TRUMPF TruTops products expose a service function without necessary authentication. Execution of this function may result in unauthorized access to change of data or disruption of the whole service.<br>**CVE ID : CVE-2022-1300** | https://cert.vde.com/en/advisories/VDE-2022-016/ | A-TRU-TRUT-200522/488 |
| **Product: trutops_monitor** | | | | | |
| Missing Authentication for Critical Function | 02-May-22 | 9.8 | Multiple Version of TRUMPF TruTops products expose a service function without necessary authentication. Execution of this function may result in unauthorized access to change of data or disruption of the whole service.<br>**CVE ID : CVE-2022-1300** | https://cert.vde.com/en/advisories/VDE-2022-016/ | A-TRU-TRUT-200522/489 |
| **Vendor: ujcms** | | | | | |
| **Product: jspxcms** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Server-Side Request Forgery (SSRF) | 04-May-22 | 6.5 | Jspxcms v10.2.0 allows attackers to execute a Server-Side Request Forgery (SSRF) via /cmscp/ext/collect/fetch_url.do?url=. **CVE ID : CVE-2022-28090** | N/A | A-UJC-JSPX-200522/490 |
| **Vendor: ureport2_project** | | | | | |
| **Product: ureport2** | | | | | |
| Deserialization of Untrusted Data | 01-May-22 | 9.8 | All versions of package com.bstek.ureport:ureport2-console are vulnerable to Remote Code Execution by connecting to a malicious database server, causing arbitrary file read and deserialization of local gadgets. **CVE ID : CVE-2022-25767** | N/A | A-URE-UREP-200522/491 |
| **Vendor: Vandyke** | | | | | |
| **Product: vshell** | | | | | |
| Improper Input Validation | 02-May-22 | 9.8 | Improper sanitization of trigger action scripts in VanDyke Software VShell for Windows v4.6.2 allows attackers to execute arbitrary code via a crafted value. **CVE ID : CVE-2022-28054** | https://www.vandyke.com/support/advisory/2022/02/remote-execution-via-triggers.html | A-VAN-VSHE-200522/492 |
| **Vendor: vendure** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: vendure** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 5.4 | In Vendure versions 0.1.0-alpha.2 to 1.5.1 are affected by Stored XSS vulnerability, where an attacker having catalog permission can upload a SVG file that contains malicious JavaScript into the "Assets" tab. The uploaded file will affect administrators as well as regular users. **CVE ID : CVE-2022-23065** | https://github.com/vendure-ecommerce/vendure/commit/69a44869112c0a5b836e2ddd3969ea9b533f51f0 | A-VEN-VEND-200522/493 |
| **Vendor: vfbpro** | | | | | |
| **Product: visual_form_builder** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-May-22 | 4.8 | The Visual Form Builder WordPress plugin before 3.0.7 does not sanitise and escape the form's 'Email to' field , which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-1046** | N/A | A-VFB-VISU-200522/494 |
| **Vendor: Webkitgtk** | | | | | |
| **Product: webkitgtk** | | | | | |
| Out-of-bounds Write | 06-May-22 | 7.5 | In WebKitGTK through 2.36.0 (and WPE WebKit), there | https://bugs.webkit.org/show_ | A-WEB-WEBK-200522/495 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | is a heap-based buffer overflow in WebCore::TextureMapperLayer::setContentsLayer in WebCore/platform/graphics/texmap/TextureMapperLayer.cpp.<br>**CVE ID : CVE-2022-30293** | bug.cgi?id=237187 | |
| Use After Free | 06-May-22 | 9.8 | In WebKitGTK through 2.36.0 (and WPE WebKit), there is a use-after-free in WebCore::TextureMapperLayer::setContentsLayer in WebCore/platform/graphics/texmap/TextureMapperLayer.cpp.<br>**CVE ID : CVE-2022-30294** | https://bugs.webkit.org/show_bug.cgi?id=237188 | A-WEB-WEBK-200522/496 |
| **Vendor: web\@rchiv_project** | | | | | |
| **Product: web\@rchiv** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 04-May-22 | 9.8 | An arbitrary file upload vulnerability in Web@rchiv 1.0 allows attackers to execute arbitrary commands via a crafted PHP file.<br>**CVE ID : CVE-2022-29347** | N/A | A-WEB-WEB\-200522/497 |
| **Vendor: wuzhicms** | | | | | |
| **Product: wuzhi_cms** | | | | | |
| Improper Neutralization of Special | 04-May-22 | 9.8 | Wuzhicms v4.1.0 was discovered to contain a SQL injection | N/A | A-WUZ-WUZH-200522/498 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an SQL Command ('SQL Injection') | | | vulnerability via the groupid parameter at /coreframe/app/member/admin/group.php.<br>**CVE ID : CVE-2022-27431** | | |
| **Vendor: Xmlsoft** | | | | | |
| **Product: libxml2** | | | | | |
| Integer Overflow or Wraparound | 03-May-22 | 6.5 | In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for integer overflows. This can result in out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software using libxml2's buffer functions, for example libxslt through 1.1.35, is affected as well.<br>**CVE ID : CVE-2022-29824** | https://gitlab.gnome.org/GNOME/libxml2/-/commit/6c283d83eccd940bcde15634ac8c7f100e3caefd, https://gitlab.gnome.org/GNOME/libxml2/-/commit/2554a2408e09f13652049e5ffb0d26196b02ebab | A-XML-LIBX-200522/499 |
| **Product: libxslt** | | | | | |
| Integer Overflow or Wraparound | 03-May-22 | 6.5 | In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for integer overflows. This can result in out-of-bounds | https://gitlab.gnome.org/GNOME/libxml2/-/commit/6c283d83eccd940bcde15634ac8c7f100e3caefd, https://gitlab.gnome.org/GNO | A-XML-LIBX-200522/500 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software using libxml2's buffer functions, for example libxslt through 1.1.35, is affected as well.<br>**CVE ID : CVE-2022-29824** | ME/libxml2/-/commit/2554a2408e09f13652049e5ffb0d26196b02ebab | |
| **Vendor: Xwiki** | | | | | |
| **Product: Xwiki** | | | | | |
| Exposure of Resource to Wrong Sphere | 02-May-22 | 7.5 | APIs to evaluate content with Velocity is a package for APIs to evaluate content with Velocity. Starting with version 2.3 and prior to 12.6.7, 12.10.3, and 13.0, the velocity scripts are not properly sandboxed against using the Java File API to perform read or write operations on the filesystem. Writing an attacking script in Velocity requires the Script rights in XWiki so not all users can use it, and it also requires finding an XWiki API which returns a File. The problem has been patched in versions 12.6.7, 12.10.3, and | https://github.com/xwiki/xwiki-commons/commit/215951cfb0f808d0bf5b1097c9e7d1e503449ab8, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-cvx5-m8vg-vxgc, https://github.com/xwiki/xwiki-commons/pull/127 | A-XWI-XWIK-200522/501 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 13.0. There is no easy workaround for fixing this vulnerability other than upgrading and being careful when giving Script rights.<br>**CVE ID : CVE-2022-24897** | | |
| **Vendor: yetiforce** | | | | | |
| **Product: yetiforce_customer_relationship_management** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 05-May-22 | 6.1 | Unrestructed file upload in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. Attacker can send malicious files to the victims is able to retrieve the stored data from the web application without that data being made safe to render in the browser and steals victim's cookie leads to account takeover.<br>**CVE ID : CVE-2022-1411** | https://huntr.dev/bounties/75c7cf09-d118-4f91-9686-22b142772529, https://github.com/yetiforcecompany/yetiforcecrm/commit/bf69c427260011ffca42f7b6935bb54080c54124 | A-YET-YETI-200522/502 |
| **Hardware** | | | | | |
| **Vendor: ABB** | | | | | |
| **Product: rtu500** | | | | | |
| Improper Input Validation | 02-May-22 | 7.5 | A vulnerability in the HCI Modbus TCP COMPONENT of Hitachi Energy RTU500 series CMU Firmware that is caused by the validation error in the length | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000103&LanguageCode=en&DocumentPartId=&Action=Launch | H-ABB-RTU5-200522/503 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information carried in MBAP header allows an ATTACKER to reboot the device by sending a special crafted message. This issue affects: Hitachi Energy RTU500 series CMU Firmware 12.0.*; 12.2.*; 12.4.*; 12.6.*; 12.7.*; 13.2.*. **CVE ID : CVE-2022-28613** | | |
| **Vendor: bdt-121_project** | | | | | |
| **Product: bdt-121** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-May-22 | 4.8 | Dragon Path Technologies Bharti Airtel Routers Hardware BDT-121 version 1.0 is vulnerable to Cross Site Scripting (XSS) via Dragon path router admin page. **CVE ID : CVE-2022-28507** | N/A | H-BDT-BDT--200522/504 |
| **Vendor: Cisco** | | | | | |
| **Product: firepower_1000** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/505 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1010** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/506 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1020** | | | | | |
| Allocation of | 03-May-22 | 7.5 | A vulnerability in the Snort detection | https://tools.cisco.com/security | H-CIS-FIRE-200522/507 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resources Without Limits or Throttling | | | engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition. | /center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1030** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/508 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1040** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/509 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1120** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/510 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1140** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/511 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_1150** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/512 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_2100** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/513 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_2110** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/514 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_2120** | | | | | |
| Allocation of Resources Without | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | H-CIS-FIRE-200522/515 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Limits or Throttling | | | (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | sa-ftd-snort-dos-hd2hFgM | |
| **Product: firepower_2130** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/516 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_2140** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/517 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4100** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/518 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4110** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/519 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4112** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/520 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4115** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/521 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4120** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/522 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4125** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/523 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4140** | | | | | |
| Allocation of Resources | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration | https://tools.cisco.com/security/center/content | H-CIS-FIRE-200522/524 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Without Limits or Throttling | | | for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition. | /CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4145** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/525 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: firepower_4150** | | | | | |
| Allocation of Resources Without Limits or Throttling | 03-May-22 | 7.5 | A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM | H-CIS-FIRE-200522/526 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20751** | | |
| **Product: rv340** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | H-CIS-RV34-200522/527 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | H-CIS-RV34-200522/528 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | H-CIS-RV34-200522/529 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | | |
| **Product: rv340w** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | H-CIS-RV34-200522/530 |
| Improper Neutralizat | 04-May-22 | 7.2 | Multiple vulnerabilities in the | https://tools.cisco.com/security | H-CIS-RV34-200522/531 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ion of Special Elements used in a Command ('Command Injection') | | | web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | /center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | |
| Improper Neutralization of | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based | https://tools.cisco.com/security/center/content | H-CIS-RV34-200522/532 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Special Elements used in a Command ('Command Injection') | | | management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | /CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | |
| **Product: rv345** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management | https://tools.cisco.com/security/center/content | H-CIS-RV34-200522/533 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | /CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | H-CIS-RV34-200522/534 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | H-CIS-RV34-200522/535 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | | |
| **Product: rv345p** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | H-CIS-RV34-200522/536 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | H-CIS-RV34-200522/537 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | H-CIS-RV34-200522/538 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | | |
| **Vendor: Dlink** | | | | | |
| **Product: dir-823_pro** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 9.8 | D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetNTPserverSeting. This vulnerability allows attackers to execute arbitrary commands via the system_time_timezone parameter.<br>**CVE ID : CVE-2022-28573** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--200522/539 |
| **Product: dir-882** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 9.8 | D-link 882 DIR882A1_FW130B06 was discovered to contain a command injection vulnerability in`/usr/bin/cli. **CVE ID : CVE-2022-28571** | https://www.dlink.com/en/security-bulletin/ | H-DLI-DIR--200522/540 |
| **Vendor: mediatek** | | | | | |
| **Product: mt6580** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/541 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/542 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/543 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/544 |
| Concurrent Execution | 03-May-22 | 6.4 | In aee driver, there is a possible use after | https://corp.mediatek.com/pro | H-MED-MT65-200522/545 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| using Shared Resource with Improper Synchronization ('Race Condition') | | | free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | duct-security-bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/546 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/547 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/548 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/549 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/550 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/551 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/552 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104. **CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/553 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could | https://corp.mediatek.com/product-security- | H-MED-MT65-200522/554 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/555 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/556 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT65-200522/557 |
| **Product: mt6731** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/558 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/559 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/560 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/561 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/562 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/563 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20091** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/564 |
| **Product: mt6732** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/565 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/566 |
| **Product: mt6735** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/567 |
| Improper Link | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic | https://corp.mediatek.com/pro | H-MED-MT67-200522/568 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | duct-security-bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/569 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/570 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/571 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/572 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/573 |
| **Product: mt6737** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/574 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/575 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. **CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/576 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/577 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/578 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/579 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6739** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/580 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/581 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/582 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/583 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/584 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/585 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/586 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/587 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/588 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/589 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/590 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/591 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/592 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/593 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/594 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/595 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/596 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/597 |
| **Product: mt6750** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/598 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/599 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/600 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/601 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/602 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/603 |
| **Product: mt6750s** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/604 |
| Improper Link | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic | https://corp.mediatek.com/pro | H-MED-MT67-200522/605 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | duct-security-bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/606 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/607 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/608 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/609 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/610 |
| **Product: mt6752** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/611 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/612 |
| **Product: mt6753** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/613 |
| Improper Link | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic | https://corp.mediatek.com/pro | H-MED-MT67-200522/614 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | duct-security-bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/615 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/616 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/617 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/618 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/619 |
| **Product: mt6755** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/620 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/621 |
| **Product: mt6755s** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/622 |
| Improper Link | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic | https://corp.mediatek.com/pro | H-MED-MT67-200522/623 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | duct-security-bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/624 |
| **Product: mt6757** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/625 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/626 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/627 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/628 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/629 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/630 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/631 |
| **Product: mt6757c** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/632 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/633 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/634 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/635 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/636 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/637 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/638 |
| **Product: mt6757cd** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/639 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/640 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/641 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/642 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/643 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/644 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/645 |
| **Product: mt6757ch** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/646 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/647 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/648 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/649 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/650 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/651 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/652 |
| **Product: mt6758** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/653 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/654 |
| **Product: mt6761** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/655 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/656 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/657 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/658 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/659 |
| Concurrent Execution | 03-May-22 | 6.4 | In aee driver, there is a possible use after | https://corp.mediatek.com/pro | H-MED-MT67-200522/660 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| using Shared Resource with Improper Synchronization ('Race Condition') | | | free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | duct-security-bulletin/May-2022 | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/661 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/662 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/663 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/664 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/665 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/666 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870. **CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/667 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405. **CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/668 |
| Improper Link Resolution Before File Access | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/669 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Link Following') | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/670 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/671 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/672 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/673 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108. **CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/674 |
| **Product: mt6762** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/675 |
| Improper Link Resolution Before File | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/676 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Access ('Link Following') | | | resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | bulletin/May-2022 | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/677 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/678 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/679 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/680 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/681 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/682 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/683 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/684 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/685 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/686 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/687 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/688 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/689 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after | https://corp.mediatek.com/pro | H-MED-MT67-200522/690 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | duct-security-bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/691 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/692 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/693 |
| **Product: mt6763** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/694 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/695 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/696 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. **CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/697 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. **CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/698 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/699 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/700 |
| **Product: mt6765** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/701 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/702 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/703 |
| Concurrent Execution using | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/704 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/705 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/706 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/707 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/708 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/709 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/710 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/711 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/712 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/713 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/714 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/715 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/716 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/717 |
| Improper Handling of | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/718 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exceptional Conditions | | | error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/719 |
| **Product: mt6768** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/720 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/721 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/722 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/723 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/724 |
| Concurrent Execution using Shared | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/725 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resource with Improper Synchronization ('Race Condition') | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | bulletin/May-2022 | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/726 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/727 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/728 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/729 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/730 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/731 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/732 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/733 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/734 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/735 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/736 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/737 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/738 |
| Improper Handling of | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/739 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exceptional Conditions | | | error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/740 |
| **Product: mt6769** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/741 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/742 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/743 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/744 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/745 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/746 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/747 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/748 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/749 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/750 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/751 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/752 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/753 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/754 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/755 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/756 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/757 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/758 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/759 |
| **Product: mt6771** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/760 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/761 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/762 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/763 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/764 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. **CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/765 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/766 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/767 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/768 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/769 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/770 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/771 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/772 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/773 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/774 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/775 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/776 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/777 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/778 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/779 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/780 |
| **Product: mt6779** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/781 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/782 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/783 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/784 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/785 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. **CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/786 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061. **CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/787 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/788 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/789 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/790 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/791 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/792 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/793 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/794 |
| Improper Limitation of a Pathname to a Restricted | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/795 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/796 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/797 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/798 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/799 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/800 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/801 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/802 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6781** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/803 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/804 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/805 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/806 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/807 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/808 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/809 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/810 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/811 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/812 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/813 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/814 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/815 |
| Improper Limitation of a | 03-May-22 | 5.5 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/816 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pathname to a Restricted Directory ('Path Traversal') | | | disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/817 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/818 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/819 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/820 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/821 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/822 |
| Integer Overflow or | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/823 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Wraparound | | | This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | bulletin/May-2022 | |
| **Product: mt6785** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/824 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/825 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/826 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/827 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/828 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/829 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/830 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/831 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/832 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/833 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/834 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/835 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/836 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/837 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | bulletin/May-2022 | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/838 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/839 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/840 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/841 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/842 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/843 |
| Improper Handling | 03-May-22 | 8.4 | In ion, there is a possible use after | https://corp.mediatek.com/pro | H-MED-MT67-200522/844 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Exceptional Conditions | | | free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | duct-security-bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/845 |
| **Product: mt6789** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/846 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/847 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/848 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/849 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/850 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/851 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/852 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/853 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/854 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/855 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| **Product: mt6795** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/856 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/857 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| **Product: mt6797** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/858 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/859 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/860 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/861 |
| Improper Handling of | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect | https://corp.mediatek.com/product-security- | H-MED-MT67-200522/862 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exceptional Conditions | | | error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/863 |
| **Product: mt6799** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/864 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT67-200522/865 |
| **Product: mt6833** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/866 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/867 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/868 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20087** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/869 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/870 |
| Concurrent Execution using Shared Resource | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/871 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| with Improper Synchronization ('Race Condition') | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/872 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/873 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/874 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/875 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763. **CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/876 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/877 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/878 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/879 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/880 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/881 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/882 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/883 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/884 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after | https://corp.mediatek.com/pro | H-MED-MT68-200522/885 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | duct-security-bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/886 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/887 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/888 |
| **Product: mt6853** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/889 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/890 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970.<br>**CVE ID : CVE-2022-20087** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/891 |
| Improper Handling | 03-May-22 | 7.8 | In aee driver, there is a possible reference | https://corp.mediatek.com/pro | H-MED-MT68-200522/892 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Exceptional Conditions | | | count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | duct-security-bulletin/May-2022 | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/893 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/894 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/895 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/896 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/897 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734. **CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/898 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/899 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/900 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/901 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/902 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/903 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/904 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/905 |
| Improper Link Resolution | 03-May-22 | 4.4 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/906 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Before File Access ('Link Following') | | | disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | bulletin/May-2022 | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/907 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/908 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/909 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/910 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/911 |
| **Product: mt6853t** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/912 |
| Improper Link | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic | https://corp.mediatek.com/pro | H-MED-MT68-200522/913 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | duct-security-bulletin/May-2022 | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/914 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/915 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/916 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/917 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061. **CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/918 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/919 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/920 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/921 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/922 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/923 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/924 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/925 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/926 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible | https://corp.mediatek.com/pro | H-MED-MT68-200522/927 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | duct-security-bulletin/May-2022 | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/928 |
| Concurrent Execution using Shared Resource with Improper Synchroniz | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/929 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ation ('Race Condition') | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/930 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/931 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-21743** | | |
| **Product: mt6873** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/932 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/933 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970. **CVE ID : CVE-2022-20087** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/934 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/935 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/936 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/937 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/938 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/939 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/940 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/941 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | bulletin/May-2022 | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/942 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/943 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/944 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/945 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/946 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/947 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405. **CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/948 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/949 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/950 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | bulletin/May-2022 | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/951 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/952 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/953 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/954 |
| **Product: mt6875** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/955 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/956 |
| Improper Handling of Exceptiona | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/957 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| l Conditions | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | bulletin/May-2022 | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/958 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/959 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/960 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/961 |
| Concurrent Execution | 03-May-22 | 4.7 | In aee daemon, there is a possible | https://corp.mediatek.com/pro | H-MED-MT68-200522/962 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| using Shared Resource with Improper Synchronization ('Race Condition') | | | information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | duct-security-bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/963 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/964 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/965 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/966 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/967 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/968 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104. **CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/969 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. **CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/970 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/971 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/972 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/973 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6877** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/974 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/975 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20085** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970.<br>**CVE ID : CVE-2022-20087** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/976 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/977 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/978 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/979 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/980 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/981 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/982 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/983 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/984 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/985 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/986 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/987 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/988 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/989 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/990 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/991 |
| Concurrent Execution using | 03-May-22 | 7 | In ion, there is a possible use after free due to a race | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/992 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | bulletin/May-2022 | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/993 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/994 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6879** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/995 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/996 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/997 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/998 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/999 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1000 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1001 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1002 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1003 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1004 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1005 |
| Improper Limitation of a Pathname to a Restricted | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1006 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1007 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1008 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1009 |
| **Product: mt6883** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1010 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1011 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1012 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1013 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1014 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1015 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1016 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1017 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1018 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1019 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1020 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1021 |
| Improper Limitation of a Pathname to a Restricted | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1022 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1023 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1024 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1025 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1026 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1027 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1028 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1029 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6885** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1030 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1031 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970.<br>**CVE ID : CVE-2022-20087** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1032 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1033 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1034 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1035 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1036 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1037 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1038 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1039 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1040 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1041 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1042 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1043 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1044 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1045 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1046 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1047 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1048 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1049 |
| Concurrent Execution using | 03-May-22 | 7 | In ion, there is a possible use after free due to a race | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/1050 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | bulletin/May-2022 | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1051 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1052 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6889** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1053 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1054 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1055 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1056 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1057 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1058 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1059 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1060 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1061 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1062 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1063 |
| Improper Limitation of a Pathname to a Restricted | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1064 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1065 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1066 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1067 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1068 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1069 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1070 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1071 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt6891** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1072 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1073 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1074 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1075 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1076 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1077 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1078 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1079 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1080 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1081 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1082 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1083 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1084 |
| Improper Link Resolution | 03-May-22 | 4.4 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/1085 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Before File Access ('Link Following') | | | disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | bulletin/May-2022 | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1086 |
| **Product: mt6893** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1087 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1088 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1089 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970.<br>**CVE ID : CVE-2022-20087** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1090 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1091 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197. **CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1092 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. **CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1093 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1094 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1095 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1096 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1097 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1098 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1099 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1100 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1101 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1102 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1103 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1104 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1105 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1106 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1107 |
| Improper Handling of | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/1108 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exceptional Conditions | | | error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1109 |
| **Product: mt6895** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1110 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1111 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1112 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1113 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1114 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/1115 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1116 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1117 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1118 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1119 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1120 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1121 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405. **CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1122 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT68-200522/1123 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access | https://corp.mediatek.com/product-security- | H-MED-MT68-200522/1124 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | bulletin/May-2022 | |
| **Product: mt6983** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1125 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1126 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1127 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1128 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1129 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1130 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving | https://corp.mediatek.com/product-security- | H-MED-MT69-200522/1131 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1132 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1133 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1134 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1135 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1136 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1137 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1138 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104. **CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1139 |
| **Product: mt6985** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving | https://corp.mediatek.com/product-security- | H-MED-MT69-200522/1140 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT69-200522/1141 |
| **Product: mt8163** | | | | | |
| Improper Handling of Exceptiona | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1142 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| l Conditions | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1143 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1144 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1145 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1146 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT81-200522/1147 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | bulletin/May-2022 | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1148 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1149 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1150 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1151 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1152 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1153 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: mt8167** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1154 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1155 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1156 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1157 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1158 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1159 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1160 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1161 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1162 |
| Improper Limitation of a Pathname to a Restricted | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1163 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1164 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1165 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1166 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1167 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1168 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1169 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1170 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt8167s** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1171 |
| **Product: mt8168** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1172 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1173 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1174 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197. **CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1175 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. **CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1176 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1177 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1178 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1179 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1180 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1181 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1182 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1183 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access | https://corp.mediatek.com/product-security- | H-MED-MT81-200522/1184 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | bulletin/May-2022 | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1185 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1186 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1187 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1188 |
| **Product: mt8173** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1189 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1190 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1191 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1192 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1193 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20091** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1194 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1195 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a | https://corp.mediatek.com/product-security- | H-MED-MT81-200522/1196 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | bulletin/May-2022 | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1197 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1198 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1199 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1200 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1201 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1202 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. **CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1203 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. **CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1204 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1205 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1206 |
| **Product: mt8175** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1207 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1208 |
| **Product: mt8183** | | | | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1209 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003. **CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1210 |
| **Product: mt8185** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1211 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1212 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1213 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1214 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1215 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1216 |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to | https://corp.mediatek.com/product-security- | H-MED-MT81-200522/1217 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1218 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1219 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1220 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1221 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1222 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1223 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1224 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104. **CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1225 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could | https://corp.mediatek.com/product-security- | H-MED-MT81-200522/1226 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1227 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1228 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT81-200522/1229 |
| **Product: mt8321** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1230 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1231 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1232 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1233 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1234 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1235 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20091** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1236 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1237 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT83-200522/1238 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | bulletin/May-2022 | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1239 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1240 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1241 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1242 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1243 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1244 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. **CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1245 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. **CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1246 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1247 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1248 |
| **Product: mt8362a** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1249 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1250 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1251 |
| Concurrent Execution using | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race | https://corp.mediatek.com/product-security- | H-MED-MT83-200522/1252 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1253 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1254 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1255 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1256 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1257 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1258 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT83-200522/1259 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | bulletin/May-2022 | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1260 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1261 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1262 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1263 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1264 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1265 |
| **Product: mt8365** | | | | | |
| Improper Link Resolution | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to | https://corp.mediatek.com/product-security- | H-MED-MT83-200522/1266 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Before File Access ('Link Following') | | | an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | bulletin/May-2022 | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1267 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1268 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1269 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1270 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1271 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1272 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1273 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1274 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1275 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1276 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1277 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1278 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1279 |
| Concurrent Execution using | 03-May-22 | 7 | In ion, there is a possible use after free due to a race | https://corp.mediatek.com/product-security- | H-MED-MT83-200522/1280 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | bulletin/May-2022 | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1281 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1282 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt8385** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1283 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1284 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003. **CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1285 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. **CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1286 |
| Concurrent Execution using Shared Resource with Improper Synchroniz | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1287 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ation ('Race Condition') | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1288 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT83-200522/1289 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-21743** | | |
| **Product: mt8666** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1290 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1291 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1292 |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003. **CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1293 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1294 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1295 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1296 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1297 |
| **Product: mt8667** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1298 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003. **CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1299 |
| **Product: mt8675** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1300 |
| Improper Link Resolution Before File | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link | https://corp.mediatek.com/product-security- | H-MED-MT86-200522/1301 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Access ('Link Following') | | | resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1302 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1303 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1304 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1305 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108. **CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1306 |
| **Product: mt8695** | | | | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397. **CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1307 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1308 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1309 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1310 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1311 |
| **Product: mt8696** | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1312 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1313 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397. **CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1314 |
| Concurrent Execution using Shared Resource with Improper Synchroniz | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1315 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ation ('Race Condition') | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1316 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1317 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20109** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1318 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1319 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT86-200522/1320 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt8735** | | | | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1321 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1322 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1323 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1324 |
| Concurrent Execution using | 03-May-22 | 4.7 | In aee daemon, there is a possible information | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1325 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Shared Resource with Improper Synchronization ('Race Condition') | | | disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1326 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1327 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1328 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1329 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1330 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1331 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1332 |
| **Product: mt8735b** | | | | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1333 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1334 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1335 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1336 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1337 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1338 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1339 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1340 |
| Improper Limitation of a Pathname to a Restricted | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1341 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Directory ('Path Traversal') | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1342 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1343 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1344 |
| **Product: mt8765** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1345 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1346 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1347 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1348 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1349 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1350 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1351 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1352 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1353 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1354 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804. **CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1355 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870. **CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1356 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1357 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1358 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1359 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1360 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1361 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1362 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1363 |
| **Product: mt8766** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1364 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1365 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1366 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1367 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1368 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. **CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1369 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868. **CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1370 |
| Concurrent Execution using Shared Resource with Improper | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1371 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Synchronization ('Race Condition') | | | disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1372 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1373 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1374 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1375 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405. **CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1376 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1377 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1378 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | bulletin/May-2022 | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1379 |
| Concurrent Execution using Shared Resource with Improper Synchronization | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1380 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Race Condition') | | | exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1381 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1382 |
| **Product: mt8768** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874. **CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1383 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1384 |
| Improper Handling of Exceptiona | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1385 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| l Conditions | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | bulletin/May-2022 | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1386 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1387 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1388 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1389 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003. **CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1390 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1391 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1392 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1393 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1394 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1395 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1396 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1397 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104. **CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1398 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1399 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1400 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1401 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1402 |
| **Product: mt8786** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1403 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1404 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1405 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1406 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1407 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1408 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20091** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1409 |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1410 |
| Concurrent Execution using Shared | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1411 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resource with Improper Synchronization ('Race Condition') | | | race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1412 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1413 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1414 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1415 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1416 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1417 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1418 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1419 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1420 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1421 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1422 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt8788** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1423 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1424 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1425 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1426 |
| Concurrent Execution using Shared Resource | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1427 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| with Improper Synchronization ('Race Condition') | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1428 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1429 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1430 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1431 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003. **CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1432 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1433 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1434 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | | |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1435 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1436 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1437 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1438 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. **CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1439 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104. **CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1440 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1441 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | bulletin/May-2022 | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1442 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1443 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1444 |
| **Product: mt8789** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1445 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. **CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1446 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201. **CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1447 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1448 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1449 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1450 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20091** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1451 |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1452 |
| Concurrent Execution using Shared | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1453 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resource with Improper Synchronization ('Race Condition') | | | race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1454 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1455 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1456 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1457 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1458 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1459 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1460 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1461 |
| Concurrent Execution using Shared Resource with | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1462 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Synchronization ('Race Condition') | | | privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1463 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1464 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt8791** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1465 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1466 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20085** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1467 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1468 |
| Concurrent Execution using Shared Resource | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1469 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| with Improper Synchronization ('Race Condition') | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1470 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1471 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1472 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1473 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1474 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442. **CVE ID : CVE-2022-20099** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1475 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1476 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1477 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1478 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1479 |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1480 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1481 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1482 |
| Improper Handling of | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1483 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exceptional Conditions | | | error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.<br>**CVE ID : CVE-2022-20111** | bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1484 |
| **Product: mt8797** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a missing permission check. This could lead to local escalation of privilege with no | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1485 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1486 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1487 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | | |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.<br>**CVE ID : CVE-2022-20089** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1488 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1489 |
| Concurrent Execution using Shared | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1490 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resource with Improper Synchronization ('Race Condition') | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | bulletin/May-2022 | |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1491 |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1492 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1493 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1494 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20095** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.<br>**CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1495 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.<br>**CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1496 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to | https://corp.mediatek.com/product-security- | H-MED-MT87-200522/1497 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | bulletin/May-2022 | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1498 |
| Improper Limitation of a Pathname to a Restricted Directory | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1499 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Path Traversal') | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1500 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1501 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: ALPS06282684.<br>**CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1502 |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1503 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901. **CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1504 |
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. **CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1505 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT87-200522/1506 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.<br>**CVE ID : CVE-2022-21743** | | |
| **Product: mt9011** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT90-200522/1507 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT90-200522/1508 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT90-200522/1509 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT90-200522/1510 |
| **Product: mt9215** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1511 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1512 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1513 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1514 |
| **Product: mt9216** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1515 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1516 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1517 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702. **CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1518 |
| **Product: mt9220** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1519 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1520 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1521 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1522 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9221** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1523 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1524 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1525 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1526 |
| **Product: mt9255** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1527 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1528 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1529 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1530 |
| **Product: mt9256** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1531 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1532 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1533 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1534 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9266** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1535 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1536 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1537 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1538 |
| **Product: mt9269** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1539 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1540 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1541 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1542 |
| **Product: mt9285** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1543 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1544 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1545 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702. **CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1546 |
| **Product: mt9286** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1547 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1548 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1549 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1550 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9288** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1551 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1552 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1553 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT92-200522/1554 |
| **Product: mt9600** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1555 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1556 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1557 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1558 |
| **Product: mt9602** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1559 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1560 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673. **CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1561 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1562 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9610** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1563 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1564 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1565 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1566 |
| **Product: mt9611** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1567 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1568 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1569 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1570 |
| **Product: mt9612** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1571 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1572 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1573 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702. **CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1574 |
| **Product: mt9613** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1575 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1576 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1577 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1578 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9615** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1579 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1580 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1581 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1582 |
| **Product: mt9617** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1583 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1584 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1585 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1586 |
| **Product: mt9629** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1587 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1588 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673. **CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1589 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1590 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9630** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1591 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1592 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1593 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1594 |
| **Product: mt9631** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1595 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1596 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1597 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1598 |
| **Product: mt9632** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1599 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1600 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1601 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1602 |
| **Product: mt9636** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1603 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1604 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1605 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1606 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9638** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1607 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1608 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1609 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1610 |
| **Product: mt9639** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1611 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1612 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1613 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1614 |
| **Product: mt9650** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1615 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1616 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673. **CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1617 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1618 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9652** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1619 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1620 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1621 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1622 |
| **Product: mt9666** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1623 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1624 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1625 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1626 |
| **Product: mt9669** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1627 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1628 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1629 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702. **CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1630 |
| **Product: mt9670** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1631 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1632 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1633 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1634 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9675** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1635 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1636 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1637 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1638 |
| **Product: mt9685** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1639 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1640 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1641 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1642 |
| **Product: mt9686** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1643 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1644 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673. **CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1645 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1646 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| **Product: mt9688** | | | | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1647 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1648 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1649 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | H-MED-MT96-200522/1650 |
| **Vendor: ruijienetworks** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: rg-nbr2100g-e** | | | | | |
| N/A | 02-May-22 | 9.8 | RG-NBR-E Enterprise Gateway RG-NBR2100G-E was discovered to contain a remote code execution (RCE) vulnerability via the fileName parameter at /guest_auth/cfg/upLoadCfg.php.<br>**CVE ID : CVE-2022-27982** | N/A | H-RUI-RG-N-200522/1651 |
| N/A | 02-May-22 | 7.5 | RG-NBR-E Enterprise Gateway RG-NBR2100G-E was discovered to contain an arbitrary file read vulnerability via the url parameter in check.php.<br>**CVE ID : CVE-2022-27983** | N/A | H-RUI-RG-N-200522/1652 |
| **Vendor: Samsung** | | | | | |
| **Product: galaxy_s22** | | | | | |
| Improper Check for Unusual or Exceptional Conditions | 03-May-22 | 4.4 | Given the TEE is compromised and controlled by the attacker, improper state maintenance in StrongBox allows attackers to change Android ROT during device boot cycle after compromising TEE. The patch is applied in Galaxy S22 to prevent change of Android ROT after first | https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=5 | H-SAM-GALA-200522/1653 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | initialization at boot time.<br>**CVE ID : CVE-2022-28793** | | |
| **Vendor: secomea** | | | | | |
| **Product: gatemanager_4250** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session.<br>**CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1654 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25779** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1655 |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1656 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session. **CVE ID : CVE-2022-25781** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1657 |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7. **CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1658 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7. **CVE ID : CVE-2022-25783** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1659 |
| Exposure of Sensitive Informatio | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET | https://www.secomea.com/sup | H-SEC-GATE-200522/1660 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n to an Unauthorized Actor | | | Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7. **CVE ID : CVE-2022-25787** | port/cybersecurity-advisory/ | |
| **Product: gatemanager_4260** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session. **CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1661 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7. **CVE ID : CVE-2022-25779** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1662 |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1663 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | logged in user to query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.<br>**CVE ID : CVE-2022-25781** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1664 |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1665 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1666 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25783** | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7. **CVE ID : CVE-2022-25787** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1667 |
| **Product: gatemanager_8250** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session. **CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1668 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1669 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25779** | | |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1670 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.<br>**CVE ID : CVE-2022-25781** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1671 |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1672 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows | https://www.secomea.com/sup | H-SEC-GATE-200522/1673 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25783** | port/cybersecurity-advisory/ | |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25787** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1674 |
| **Product: gatemanager_9250** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session.<br>**CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1675 |
| Uncontrolled Resource | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1676 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25779** | | |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1677 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.<br>**CVE ID : CVE-2022-25781** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1678 |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1679 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25782** | | |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25783** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1680 |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25787** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-GATE-200522/1681 |
| **Product: sitemanager_1129** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1682 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25784** | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1683 |
| **Product: sitemanager_1139** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1684 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1685 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: sitemanager_1149** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1686 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1687 |
| **Product: sitemanager_3329** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1688 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1689 |
| **Product: sitemanager_3339** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1690 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1691 |
| **Product: sitemanager_3349** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1692 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1693 |
| **Product: sitemanager_3529** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1694 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows | https://www.secomea.com/sup | H-SEC-SITE-200522/1695 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | port/cybersecurity-advisory/ | |
| **Product: sitemanager_3539** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1696 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1697 |
| **Product: sitemanager_3549** | | | | | |
| Improper Neutralization of Input During | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1698 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | H-SEC-SITE-200522/1699 |
| **Vendor: tanda** | | | | | |
| **Product: ax1803** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 8.8 | Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability in `SetIPv6Status` function **CVE ID : CVE-2022-28572** | N/A | H-TAN-AX18-200522/1700 |
| **Product: ax1806** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Comman | 02-May-22 | 8.8 | Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability in `SetIPv6Status` function | N/A | H-TAN-AX18-200522/1701 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| d Injection') | | | **CVE ID : CVE-2022-28572** | | |
| **Vendor: Tenda** | | | | | |
| **Product: ac15** | | | | | |
| Allocation of Resources Without Limits or Throttling | 04-May-22 | 7.5 | Tenda AC15 US_AC15V1.0BR_V15.03.05.20_multi_TDE01.bin is vulnerable to Buffer Overflow. The stack overflow vulnerability lies in the /goform/setpptpservercfg interface of the web. The sent post data startip and endip are copied to the stack using the sanf function, resulting in stack overflow. Similarly, this vulnerability can be used together with CVE-2021-44971<br>**CVE ID : CVE-2022-28556** | N/A | H-TEN-AC15-200522/1702 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 9.8 | There is a command injection vulnerability at the /goform/setsambacfg interface of Tenda AC15 US_AC15V1.0BR_V15.03.05.20_multi_TDE01.bin device web, which can also cooperate with CVE-2021-44971 to cause unconditional arbitrary command execution | N/A | H-TEN-AC15-200522/1703 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28557** | | |
| **Product: ac9** | | | | | |
| Out-of-bounds Write | 03-May-22 | 9.8 | There is a stack overflow vulnerability in the goform/fast_setting_wifi_set function in the httpd service of Tenda ac9 15.03.2.21_cn router. An attacker can obtain a stable shell through a carefully constructed payload **CVE ID : CVE-2022-28560** | N/A | H-TEN-AC9-200522/1704 |
| **Product: ax12** | | | | | |
| Out-of-bounds Write | 04-May-22 | 9.8 | Tenda AX12 v22.03.01.21_CN was discovered to contain a stack overflow via the list parameter at /goform/SetNetControlList. **CVE ID : CVE-2022-28082** | N/A | H-TEN-AX12-200522/1705 |
| Out-of-bounds Write | 03-May-22 | 9.8 | There is a stack overflow vulnerability in the /goform/setMacFilterCfg function in the httpd service of Tenda ax12 22.03.01.21_cn router. An attacker can obtain a stable shell through a carefully constructed payload | N/A | H-TEN-AX12-200522/1706 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28561** | | |
| **Product: tx9_pro** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 05-May-22 | 9.8 | Tenda TX9 Pro 22.03.02.10 devices allow OS command injection via set_route (called by doSystemCmd_route ). **CVE ID : CVE-2022-29592** | N/A | H-TEN-TX9_-200522/1707 |
| **Vendor: totolink** | | | | | |
| **Product: a7100ru** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setopenvpnclientcfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows attackers to execute arbitrary commands through a carefully constructed payload **CVE ID : CVE-2022-28575** | N/A | H-TOT-A710-200522/1708 |
| Improper Neutralization of Special Elements used in a Command ('Comman | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the delParentalRules interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to | N/A | H-TOT-A710-200522/1709 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| d Injection') | | | execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28577** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setOpenVpnCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28578** | N/A | H-TOT-A710-200522/1710 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setParentalRules interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28579** | N/A | H-TOT-A710-200522/1711 |
| Improper Neutralization of Special | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the | N/A | H-TOT-A710-200522/1712 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in a Command ('Command Injection') | | | setL2tpServerCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28580** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiAdvancedCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28581** | N/A | H-TOT-A710-200522/1713 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiSignalCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload. | N/A | H-TOT-A710-200522/1714 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28582** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiWpsCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28583** | N/A | H-TOT-A710-200522/1715 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiWpsStart interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28584** | N/A | H-TOT-A710-200522/1716 |
| **Product: n600r** | | | | | |
| Improper Neutralization of Special Elements used in a Command | 05-May-22 | 9.8 | TOTOLINK N600R v5.3c.5507_B20171031 was discovered to contain a command injection vulnerability via the QUERY_STRING | N/A | H-TOT-N600-200522/1717 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Command Injection') | | | parameter in the "Main" function.<br>**CVE ID : CVE-2022-27411** | | |
| **Operating System** | | | | | |
| **Vendor: ABB** | | | | | |
| **Product: rtu500_firmware** | | | | | |
| Improper Input Validation | 02-May-22 | 7.5 | A vulnerability in the HCI Modbus TCP COMPONENT of Hitachi Energy RTU500 series CMU Firmware that is caused by the validation error in the length information carried in MBAP header allows an ATTACKER to reboot the device by sending a special crafted message. This issue affects: Hitachi Energy RTU500 series CMU Firmware 12.0.*; 12.2.*; 12.4.*; 12.6.*; 12.7.*; 13.2.*.<br>**CVE ID : CVE-2022-28613** | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000103&LanguageCode=en&DocumentPartId=&Action=Launch | O-ABB-RTU5-230522/1718 |
| **Vendor: Apple** | | | | | |
| **Product: macos** | | | | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1719 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 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-2022-23205** | | |
| Improper Input Validation | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an improper input validation vulnerability when parsing a PCX file 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 PCX file.<br>**CVE ID : CVE-2022-24098** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1720 |
| Out-of-bounds Read | 06-May-22 | 3.3 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1721 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 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-2022-24099** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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 U3D file.<br>**CVE ID : CVE-2022-24105** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1722 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. | https://helpx.adobe.com/security/products/after_effects/apsb22-19.html | O-APP-MACO-230522/1723 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Exploitation requires user interaction in that a victim must open a crafted file in After Effects.<br>**CVE ID : CVE-2022-27783** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack 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 After Effects.<br>**CVE ID : CVE-2022-27784** | https://helpx.adobe.com/security/products/after_effects/apsb22-19.html | O-APP-MACO-230522/1724 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1725 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | victim must open a malicious SVG file.<br>**CVE ID : CVE-2022-28270** | | |
| Use After Free | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by a use-after-free 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 PDF file.<br>**CVE ID : CVE-2022-28271** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1726 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28272** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1727 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28273** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1728 |
| Out-of-bounds Read | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1729 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28274** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28275** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1730 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28276** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1731 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 PDF file. **CVE ID : CVE-2022-28277** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-APP-MACO-230522/1732 |
| **Vendor: bdt-121_project** | | | | | |
| **Product: bdt-121_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-May-22 | 4.8 | Dragon Path Technologies Bharti Airtel Routers Hardware BDT-121 version 1.0 is vulnerable to Cross Site Scripting (XSS) via Dragon path router admin page. **CVE ID : CVE-2022-28507** | N/A | O-BDT-BDT--230522/1733 |
| **Vendor: Cisco** | | | | | |
| **Product: adaptive_security_appliance_software** | | | | | |
| Improper Input Validation | 03-May-22 | 7.5 | A vulnerability in the remote access SSL VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA | O-CIS-ADAP-230522/1734 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper validation of errors that are logged as a result of client connections that are made using remote access VPN. An attacker could exploit this vulnerability by sending crafted requests to an affected system. A successful exploit could allow the attacker to cause the affected device to restart, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20715** | | |
| Out-of-bounds Write | 03-May-22 | 7.1 | A vulnerability in the handler for HTTP authentication for resources accessed through the Clientless SSL VPN portal of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-heap-zLX3FdX | O-CIS-ADAP-230522/1735 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | service (DoS) condition on an affected device or to obtain portions of process memory from an affected device. This vulnerability is due to insufficient bounds checking when parsing specific HTTP authentication messages. An attacker could exploit this vulnerability by sending malicious traffic to an affected device acting as a VPN Gateway. To send this malicious traffic, an attacker would need to control a web server that can be accessed through the Clientless SSL VPN portal. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition, or to retrieve bytes from the device process memory that may contain sensitive information.<br>**CVE ID : CVE-2022-20737** | | |
| N/A | 03-May-22 | 7.4 | A vulnerability in an IPsec VPN library of | https://tools.cisco.com/security | O-CIS-ADAP-230522/1736 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to read or modify data within an IPsec IKEv2 VPN tunnel. This vulnerability is due to an improper implementation of Galois/Counter Mode (GCM) ciphers. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a sufficient number of encrypted messages across an affected IPsec IKEv2 VPN tunnel and then using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to decrypt, read, modify, and re-encrypt data that is transmitted across an affected IPsec IKEv2 VPN tunnel.<br>**CVE ID : CVE-2022-20742** | /center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ipsec-mitm-CKnLr4 | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-May-22 | 7.5 | A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper input validation when parsing HTTPS requests. An attacker could exploit this vulnerability by sending a crafted HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20745** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-tzPSYern | O-CIS-ADAP-230522/1737 |
| Improper Privilege Management | 03-May-22 | 8.8 | A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye | O-CIS-ADAP-230522/1738 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (FTD) Software could allow an authenticated, but unprivileged, remote attacker to elevate privileges to level 15. This vulnerability is due to improper separation of authentication and authorization scopes. An attacker could exploit this vulnerability by sending crafted HTTPS messages to the web services interface of an affected device. A successful exploit could allow the attacker to gain privilege level 15 access to the web management interface of the device. This includes privilege level 15 access to the device using management tools like the Cisco Adaptive Security Device Manager (ASDM) or the Cisco Security Manager (CSM). Note: With Cisco FTD Software, the impact is lower than the CVSS score suggests because the affected web management interface allows for read access only. | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20759** | | |
| Uncontrolled Resource Consumption | 03-May-22 | 7.5 | A vulnerability in the DNS inspection handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service condition (DoS) on an affected device. This vulnerability is due to a lack of proper processing of incoming requests. An attacker could exploit this vulnerability by sending crafted DNS requests at a high rate to an affected device. A successful exploit could allow the attacker to cause the device to stop responding, resulting in a DoS condition.<br>**CVE ID : CVE-2022-20760** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-nJVAwOeq | O-CIS-ADAP-230522/1739 |
| **Product: roomos** | | | | | |
| N/A | 04-May-22 | 8.1 | Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | O-CIS-ROOM-230522/1740 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software and Cisco RoomOS Software could allow a remote attacker to cause a denial of service (DoS) condition, view sensitive data on an affected device, or redirect users to an attacker-controlled destination. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2022-20764** | sa-ROS-DOS-X7H7XhkK | |
| URL Redirection to Untrusted Site ('Open Redirect') | 04-May-22 | 4.7 | Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow a remote attacker to cause a denial of service (DoS) condition, view sensitive data on an affected device, or redirect users to an attacker-controlled destination. For more information about these vulnerabilities, see the Details section of this advisory. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ROS-DOS-X7H7XhkK | O-CIS-ROOM-230522/1741 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20794** | | |
| **Product: rv340w_firmware** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | O-CIS-RV34-230522/1742 |
| Improper Neutralization of Special Elements | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | O-CIS-RV34-230522/1743 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in a Command ('Command Injection') | | | Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | sa-smb-rv-cmd-inj-8Pv9JMJD | |
| Improper Neutralization of Special Elements used in a | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | O-CIS-RV34-230522/1744 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('Command Injection') | | | RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | sa-smb-rv-cmd-inj-8Pv9JMJD | |
| **Product: rv340_firmware** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco- | O-CIS-RV34-230522/1745 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | sa-sbrv-rce-OYLQbL9u | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | O-CIS-RV34-230522/1746 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | O-CIS-RV34-230522/1747 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | | |
| **Product: rv345p_firmware** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user- | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | O-CIS-RV34-230522/1748 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | O-CIS-RV34-230522/1749 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | O-CIS-RV34-230522/1750 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | | |
| **Product: rv345_firmware** | | | | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | A vulnerability in web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to an affected device. A successful exploit could allow the attacker to | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u | O-CIS-RV34-230522/1751 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execute remote code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20753** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | O-CIS-RV34-230522/1752 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20799** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 04-May-22 | 7.2 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340 and RV345 Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system of the affected device. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD | O-CIS-RV34-230522/1753 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.<br>**CVE ID : CVE-2022-20801** | | |
| **Vendor: Dlink** | | | | | |
| **Product: dir-823_pro_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 9.8 | D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetNTPserverSeting. This vulnerability allows attackers to execute arbitrary commands via the system_time_timezone parameter.<br>**CVE ID : CVE-2022-28573** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--230522/1754 |
| **Product: dir-882_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 9.8 | D-link 882 DIR882A1_FW130B06 was discovered to contain a command injection vulnerability in`/usr/bin/cli.<br>**CVE ID : CVE-2022-28571** | https://www.dlink.com/en/security-bulletin/ | O-DLI-DIR--230522/1755 |
| **Vendor: Fedoraproject** | | | | | |
| **Product: fedora** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 04-May-22 | 7.8 | SDL_ttf v2.0.18 and below was discovered to contain an arbitrary memory write via the function TTF_RenderText_Solid(). This vulnerability is triggered via a crafted TTF file. **CVE ID : CVE-2022-27470** | https://github.com/libsdl-org/SDL_ttf/commit/db1b41ab8bde6723c24b866e466cad78c2fa0448, https://github.com/libsdl-org/SDL_ttf/issues/187 | O-FED-FEDO-230522/1756 |
| Integer Overflow or Wraparound | 03-May-22 | 6.5 | In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for integer overflows. This can result in out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software using libxml2's buffer functions, for example libxslt through 1.1.35, is affected as well. **CVE ID : CVE-2022-29824** | https://gitlab.gnome.org/GNOME/libxml2/-/commit/6c283d83eccd940bcde15634ac8c7f100e3caefd, https://gitlab.gnome.org/GNOME/libxml2/-/commit/2554a2408e09f13652049e5ffb0d26196b02ebab | O-FED-FEDO-230522/1757 |
| **Vendor: Google** | | | | | |
| **Product: android** | | | | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving emergency broadcasts due to a | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1758 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498874; Issue ID: ALPS06498874.<br>**CVE ID : CVE-2022-20084** | | |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 6.7 | In netdiag, there is a possible symbolic link following due to an improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06308877; Issue ID: ALPS06308877.<br>**CVE ID : CVE-2022-20085** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1759 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1760 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970.<br>**CVE ID : CVE-2022-20087** | | |
| Improper Handling of Exceptional Conditions | 03-May-22 | 7.8 | In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.<br>**CVE ID : CVE-2022-20088** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1761 |
| N/A | 03-May-22 | 6.7 | In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397. | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1762 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20089** | | |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.<br>**CVE ID : CVE-2022-20090** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1763 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 6.4 | In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.<br>**CVE ID : CVE-2022-20091** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1764 |
| Out-of-bounds Read | 03-May-22 | 5.5 | In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1765 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.<br>**CVE ID : CVE-2022-20092** | | |
| Missing Authorization | 03-May-22 | 7.8 | In telephony, there is a possible way to disable receiving SMS messages due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06498868; Issue ID: ALPS06498868.<br>**CVE ID : CVE-2022-20093** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1766 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1767 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.<br>**CVE ID : CVE-2022-20094** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.<br>**CVE ID : CVE-2022-20095** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1768 |
| Use of Uninitialized Resource | 03-May-22 | 4.4 | In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.<br>**CVE ID : CVE-2022-20096** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1769 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 4.7 | In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944. **CVE ID : CVE-2022-20097** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1770 |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017. **CVE ID : CVE-2022-20098** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1771 |
| Out-of-bounds Write | 03-May-22 | 7.8 | In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1772 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.<br>**CVE ID : CVE-2022-20099** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.<br>**CVE ID : CVE-2022-20100** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1773 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1774 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.<br>**CVE ID : CVE-2022-20101** | | |
| Missing Authorization | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.<br>**CVE ID : CVE-2022-20102** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1775 |
| Improper Link Resolution Before File Access ('Link Following') | 03-May-22 | 4.4 | In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684. | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1776 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-20103** | | |
| N/A | 03-May-22 | 5.5 | In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.<br>**CVE ID : CVE-2022-20104** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1777 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1778 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to | https://corp.mediatek.com/product-security- | O-GOO-ANDR-230522/1779 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.<br>**CVE ID : CVE-2022-20106** | bulletin/May-2022 | |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1780 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1781 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | | |
| Use After Free | 03-May-22 | 7.8 | In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.<br>**CVE ID : CVE-2022-20109** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1782 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 03-May-22 | 7 | In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.<br>**CVE ID : CVE-2022-20110** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1783 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Handling of Exceptional Conditions | 03-May-22 | 8.4 | In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069. **CVE ID : CVE-2022-20111** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1784 |
| Integer Overflow or Wraparound | 03-May-22 | 7.8 | In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108. **CVE ID : CVE-2022-21743** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-GOO-ANDR-230522/1785 |
| N/A | 03-May-22 | 5.5 | Improper access control vulnerability in Weather prior to SMR May-2022 Release 1 allows that attackers can access location information that set in Weather without permission. | N/A | O-GOO-ANDR-230522/1786 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | The patch adds proper protection to prevent access to location information.<br>**CVE ID : CVE-2022-28780** | | |
| Improper Input Validation | 03-May-22 | 6.7 | Improper input validation in Settings prior to SMR-May-2022 Release 1 allows attackers to launch arbitrary activity with system privilege. The patch adds proper validation logic to check the caller.<br>**CVE ID : CVE-2022-28781** | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1787 |
| Incorrect Authorization | 03-May-22 | 4.6 | Improper access control vulnerability in Contents To Window prior to SMR May-2022 Release 1 allows physical attacker to install package before completion of Setup wizard. The patch blocks entry point of the vulnerability.<br>**CVE ID : CVE-2022-28782** | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1788 |
| Improper Input Validation | 03-May-22 | 7.1 | Improper validation of removing package name in Galaxy Themes prior to SMR May-2022 Release 1 allows attackers to uninstall arbitrary packages without | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1789 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | permission. The patch adds proper validation logic for removing package name.<br>**CVE ID : CVE-2022-28783** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-May-22 | 3.3 | Path traversal vulnerability in Galaxy Themes prior to SMR May-2022 Release 1 allows attackers to list file names in arbitrary directory as system user. The patch addresses incorrect implementation of file path validation check logic.<br>**CVE ID : CVE-2022-28784** | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1790 |
| Out-of-bounds Read | 03-May-22 | 5.5 | Improper buffer size check logic in aviextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.<br>**CVE ID : CVE-2022-28785** | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1791 |
| Out-of-bounds Read | 03-May-22 | 5.5 | Improper buffer size check logic in aviextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1792 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | possible temporary denial of service. The patch adds buffer size check logic.<br>**CVE ID : CVE-2022-28786** | | |
| Out-of-bounds Read | 03-May-22 | 5.5 | Improper buffer size check logic in wmfextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.<br>**CVE ID : CVE-2022-28787** | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1793 |
| Out-of-bounds Read | 03-May-22 | 5.5 | Improper buffer size check logic in aviextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.<br>**CVE ID : CVE-2022-28788** | https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=5 | O-GOO-ANDR-230522/1794 |
| **Product: fuchsia** | | | | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 03-May-22 | 5.5 | A bug exists where an attacker can read the kernel log through exposed Zircon kernel addresses without the required capability ZX_RSRC_KIND_ROO | https://bugs.fuchsia.dev/p/fuchsia/issues/detail?id=94740 | O-GOO-FUCH-230522/1795 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | T. It is recommended to upgrade the Fuchsia kernel to 4.1.1 or greater.<br>**CVE ID : CVE-2022-0882** | | |
| **Vendor: IBM** | | | | | |
| **Product: aix** | | | | | |
| Inadequate Encryption Strength | 03-May-22 | 7.5 | IBM Spectrum Scale 5.1.0 through 5.1.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 221012.<br>**CVE ID : CVE-2022-22368** | https://exchange.xforce.ibmcloud.com/vulnerabilities/221012, https://www.ibm.com/support/pages/node/6579139 | O-IBM-AIX-230522/1796 |
| **Vendor: Linux** | | | | | |
| **Product: linux_kernel** | | | | | |
| Use After Free | 05-May-22 | 5.5 | A NULL pointer dereference flaw was found in the Linux kernel's X.25 set of standardized network protocols functionality in the way a user terminates their session using a simulated Ethernet card and continued usage of this connection. This flaw allows a local user to crash the system.<br>**CVE ID : CVE-2022-1516** | https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=7781607938c8 | O-LIN-LINU-230522/1797 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20105** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-LIN-LINU-230522/1798 |
| Out-of-bounds Write | 03-May-22 | 6.7 | In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460. **CVE ID : CVE-2022-20106** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-LIN-LINU-230522/1799 |
| Integer Overflow or Wraparound | 03-May-22 | 4.4 | In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-LIN-LINU-230522/1800 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.<br>**CVE ID : CVE-2022-20107** | | |
| Out-of-bounds Write | 03-May-22 | 6.7 | In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.<br>**CVE ID : CVE-2022-20108** | https://corp.mediatek.com/product-security-bulletin/May-2022 | O-LIN-LINU-230522/1801 |
| Inadequate Encryption Strength | 03-May-22 | 7.5 | IBM Spectrum Scale 5.1.0 through 5.1.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 221012.<br>**CVE ID : CVE-2022-22368** | https://exchange.xforce.ibmcloud.com/vulnerabilities/221012, https://www.ibm.com/support/pages/node/6579139 | O-LIN-LINU-230522/1802 |
| **Vendor: Microsoft** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: windows** | | | | | |
| Inadequate Encryption Strength | 03-May-22 | 7.5 | IBM Spectrum Scale 5.1.0 through 5.1.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 221012. **CVE ID : CVE-2022-22368** | https://exchange.xforce.ibmcloud.com/vulnerabilities/221012, https://www.ibm.com/support/pages/node/6579139 | O-MIC-WIND-230522/1803 |
| N/A | 05-May-22 | 6.5 | A vulnerability exists where an IBM Robotic Process Automation 21.0.1 regular user is able to obtain view-only access to some admin pages in the Control Center IBM X-Force ID: 223029. **CVE ID : CVE-2022-22415** | https://www.ibm.com/support/pages/node/6570235, https://exchange.xforce.ibmcloud.com/vulnerabilities/223029 | O-MIC-WIND-230522/1804 |
| N/A | 05-May-22 | 4.6 | IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with physical access to create an API request modified to create additional objects. IBM X-Force ID: 224159. **CVE ID : CVE-2022-22434** | https://exchange.xforce.ibmcloud.com/vulnerabilities/224159, https://www.ibm.com/support/pages/node/6579959 | O-MIC-WIND-230522/1805 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are | https://helpx.adobe.com/security/products/p | O-MIC-WIND-230522/1806 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 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-2022-23205** | hotoshop/apsb22-20.html | |
| Improper Input Validation | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an improper input validation vulnerability when parsing a PCX file 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 PCX file.<br>**CVE ID : CVE-2022-24098** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1807 |
| Out-of-bounds Read | 06-May-22 | 3.3 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by an out-of-bounds read vulnerability that | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1808 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 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-2022-24099** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (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 U3D file.<br>**CVE ID : CVE-2022-24105** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1809 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack overflow vulnerability due to insecure handling of a crafted file, | https://helpx.adobe.com/security/products/after_effects/apsb22-19.html | O-MIC-WIND-230522/1810 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 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 After Effects.<br>**CVE ID : CVE-2022-27783** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe After Effects versions 22.2.1 (and earlier) and 18.4.5 (and earlier) are affected by a stack 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 After Effects.<br>**CVE ID : CVE-2022-27784** | https://helpx.adobe.com/security/products/after_effects/apsb22-19.html | O-MIC-WIND-230522/1811 |
| Improper Input Validation | 02-May-22 | 9.8 | Improper sanitization of trigger action scripts in VanDyke Software VShell for Windows v4.6.2 allows attackers to execute arbitrary code via a crafted value. | https://www.vandyke.com/support/advisory/2022/02/remote-execution-via-triggers.html | O-MIC-WIND-230522/1812 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-28054** | | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 SVG file.<br>**CVE ID : CVE-2022-28270** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1813 |
| Use After Free | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier)and 23.2.2 (and earlier) are affected by a use-after-free 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 PDF file.<br>**CVE ID : CVE-2022-28271** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1814 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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. **CVE ID : CVE-2022-28272** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1815 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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. **CVE ID : CVE-2022-28273** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1816 |
| Out-of-bounds Read | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (and earlier) are affected by an out-of- | https://helpx.adobe.com/security/products/p | O-MIC-WIND-230522/1817 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2022-28274** | hotoshop/apsb22-20.html | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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-2022-28275** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1818 |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (and earlier) are | https://helpx.adobe.com/security/products/p | O-MIC-WIND-230522/1819 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 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-2022-28276** | hotoshop/apsb22-20.html | |
| Out-of-bounds Write | 06-May-22 | 7.8 | Adobe Photoshop versions 22.5.6 (and earlier) and 23.2.2 (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 PDF file.<br>**CVE ID : CVE-2022-28277** | https://helpx.adobe.com/security/products/photoshop/apsb22-20.html | O-MIC-WIND-230522/1820 |
| **Vendor: ruijienetworks** | | | | | |
| **Product: rg-nbr2100g-e_firmware** | | | | | |
| N/A | 02-May-22 | 9.8 | RG-NBR-E Enterprise Gateway RG-NBR2100G-E was discovered to contain a remote code execution | N/A | O-RUI-RG-N-230522/1821 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (RCE) vulnerability via the fileName parameter at /guest_auth/cfg/upLoadCfg.php.<br>**CVE ID : CVE-2022-27982** | | |
| N/A | 02-May-22 | 7.5 | RG-NBR-E Enterprise Gateway RG-NBR2100G-E was discovered to contain an arbitrary file read vulnerability via the url parameter in check.php.<br>**CVE ID : CVE-2022-27983** | N/A | O-RUI-RG-N-230522/1822 |
| **Vendor: Samsung** | | | | | |
| **Product: galaxy_s22_firmware** | | | | | |
| Improper Check for Unusual or Exceptional Conditions | 03-May-22 | 4.4 | Given the TEE is compromised and controlled by the attacker, improper state maintenance in StrongBox allows attackers to change Android ROT during device boot cycle after compromising TEE. The patch is applied in Galaxy S22 to prevent change of Android ROT after first initialization at boot time.<br>**CVE ID : CVE-2022-28793** | https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=5 | O-SAM-GALA-230522/1823 |
| **Vendor: secomea** | | | | | |
| **Product: gatemanager_4250_firmware** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session. **CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1824 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7. **CVE ID : CVE-2022-25779** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1825 |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope. **CVE ID : CVE-2022-25780** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1826 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session. | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1827 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25781** | | |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1828 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25783** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1829 |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1830 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Secomea GateManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25787** | | |
| **Product: gatemanager_4260_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session.<br>**CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1831 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25779** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1832 |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1833 |
| Improper Neutralizat | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in | https://www.secomea.com/sup | O-SEC-GATE-230522/1834 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ion of Input During Web Page Generation ('Cross-site Scripting') | | | Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.<br>**CVE ID : CVE-2022-25781** | port/cybersecurity-advisory/ | |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1835 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25783** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1836 |
| Exposure of Sensitive Information to an | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1837 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unauthorized Actor | | | API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7. **CVE ID : CVE-2022-25787** | | |
| **Product: gatemanager_8250_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session. **CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1838 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7. **CVE ID : CVE-2022-25779** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1839 |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1840 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.<br>**CVE ID : CVE-2022-25781** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1841 |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1842 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1843 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25783** | | |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25787** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1844 |
| **Product: gatemanager_9250_firmware** | | | | | |
| Cross-Site Request Forgery (CSRF) | 04-May-22 | 8.8 | Cross-Site Request Forgery (CSRF) vulnerability in Web UI of Secomea GateManager allows phishing attacker to issue get request in logged in user session.<br>**CVE ID : CVE-2022-25778** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1845 |
| Uncontrolled Resource Consumption | 04-May-22 | 4.3 | Logging of Excessive Data vulnerability in audit log of Secomea GateManager allows logged in user to write text entries in audit log. This issue affects: Secomea GateManager versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1846 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25779** | | |
| N/A | 04-May-22 | 4.3 | Information Exposure vulnerability in web UI of Secomea GateManager allows logged in user to query devices outside own scope.<br>**CVE ID : CVE-2022-25780** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1847 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 6.1 | Cross-site Scripting (XSS) vulnerability in Web UI of Secomea GateManager allows phishing attacker to inject javascript or html into logged in user session.<br>**CVE ID : CVE-2022-25781** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1848 |
| Improper Privilege Management | 04-May-22 | 5.4 | Improper Handling of Insufficient Privileges vulnerability in Web UI of Secomea GateManager allows logged in user to access and update privileged information. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25782** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1849 |
| N/A | 04-May-22 | 4.3 | Insufficient Logging vulnerability in web server of Secomea GateManager allows | https://www.secomea.com/sup | O-SEC-GATE-230522/1850 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | logged in user to issue improper queries without logging. This issue affects: Secomea GateManager versions prior to 9.7.<br>**CVE ID : CVE-2022-25783** | port/cybersecurity-advisory/ | |
| Exposure of Sensitive Information to an Unauthorized Actor | 04-May-22 | 6.7 | Information Exposure Through Query Strings in GET Request vulnerability in LMM API of Secomea GateManager allows system administrator to hijack connection. This issue affects: Secomea GateManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25787** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-GATE-230522/1851 |
| **Product: sitemanager_1129_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1852 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows | https://www.secomea.com/sup | O-SEC-SITE-230522/1853 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | port/cybersecurity-advisory/ | |
| **Product: sitemanager_1139_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1854 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1855 |
| **Product: sitemanager_1149_firmware** | | | | | |
| Improper Neutralization of Input During | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1856 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Web Page Generation ('Cross-site Scripting') | | | inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1857 |
| **Product: sitemanager_3329_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1858 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1859 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | | |
| **Product: sitemanager_3339_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1860 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1861 |
| **Product: sitemanager_3349_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1862 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2022-25784** | | |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1863 |
| **Product: sitemanager_3529_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1864 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7.<br>**CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1865 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: sitemanager_3539_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1866 |
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1867 |
| **Product: sitemanager_3549_firmware** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-May-22 | 4.8 | Cross-site Scripting (XSS) vulnerability in Web GUI of SiteManager allows logged-in user to inject scripting. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25784** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1868 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 04-May-22 | 7.2 | Stack-based Buffer Overflow vulnerability in SiteManager allows logged-in or local user to cause arbitrary code execution. This issue affects: Secomea SiteManager all versions prior to 9.7. **CVE ID : CVE-2022-25785** | https://www.secomea.com/support/cybersecurity-advisory/ | O-SEC-SITE-230522/1869 |
| **Vendor: tanda** | | | | | |
| **Product: ax1803_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 8.8 | Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability in `SetIPv6Status` function **CVE ID : CVE-2022-28572** | N/A | O-TAN-AX18-230522/1870 |
| **Product: ax1806_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 02-May-22 | 8.8 | Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability in `SetIPv6Status` function **CVE ID : CVE-2022-28572** | N/A | O-TAN-AX18-230522/1871 |
| **Vendor: Tenda** | | | | | |
| **Product: ac15_firmware** | | | | | |
| Allocation of | 04-May-22 | 7.5 | Tenda AC15 US_AC15V1.0BR_V15 | N/A | O-TEN-AC15-230522/1872 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resources Without Limits or Throttling | | | .03.05.20_multi_TDE 01.bin is vulnerable to Buffer Overflow. The stack overflow vulnerability lies in the /goform/setpptpser vercfg interface of the web. The sent post data startip and endip are copied to the stack using the sanf function, resulting in stack overflow. Similarly, this vulnerability can be used together with CVE-2021-44971<br>**CVE ID : CVE-2022-28556** | | |
| Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection') | 04-May-22 | 9.8 | There is a command injection vulnerability at the /goform/setsambacf g interface of Tenda AC15 US_AC15V1.0BR_V15 .03.05.20_multi_TDE 01.bin device web, which can also cooperate with CVE-2021-44971 to cause unconditional arbitrary command execution<br>**CVE ID : CVE-2022-28557** | N/A | O-TEN-AC15-230522/1873 |
| **Product: ac9_firmware** | | | | | |
| Out-of-bounds Write | 03-May-22 | 9.8 | There is a stack overflow vulnerability in the | N/A | O-TEN-AC9_-230522/1874 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | goform/fast_setting_wifi_set function in the httpd service of Tenda ac9 15.03.2.21_cn router. An attacker can obtain a stable shell through a carefully constructed payload **CVE ID : CVE-2022-28560** | | |
| **Product: ax12_firmware** | | | | | |
| Out-of-bounds Write | 04-May-22 | 9.8 | Tenda AX12 v22.03.01.21_CN was discovered to contain a stack overflow via the list parameter at /goform/SetNetControlList. **CVE ID : CVE-2022-28082** | N/A | O-TEN-AX12-230522/1875 |
| Out-of-bounds Write | 03-May-22 | 9.8 | There is a stack overflow vulnerability in the /goform/setMacFilterCfg function in the httpd service of Tenda ax12 22.03.01.21_cn router. An attacker can obtain a stable shell through a carefully constructed payload **CVE ID : CVE-2022-28561** | N/A | O-TEN-AX12-230522/1876 |
| **Product: tx9_pro_firmware** | | | | | |
| Improper Neutralization of | 05-May-22 | 9.8 | Tenda TX9 Pro 22.03.02.10 devices allow OS command | N/A | O-TEN-TX9_-230522/1877 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Special Elements used in an OS Command ('OS Command Injection') | | | injection via set_route (called by doSystemCmd_route ).<br>**CVE ID : CVE-2022-29592** | | |
| **Vendor: totolink** | | | | | |
| **Product: a7100ru_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setopenvpnclientcfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows attackers to execute arbitrary commands through a carefully constructed payload<br>**CVE ID : CVE-2022-28575** | N/A | O-TOT-A710-230522/1878 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the delParentalRules interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28577** | N/A | O-TOT-A710-230522/1879 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setOpenVpnCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload. **CVE ID : CVE-2022-28578** | N/A | O-TOT-A710-230522/1880 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setParentalRules interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload. **CVE ID : CVE-2022-28579** | N/A | O-TOT-A710-230522/1881 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setL2tpServerCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary | N/A | O-TOT-A710-230522/1882 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28580** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiAdvancedCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28581** | N/A | O-TOT-A710-230522/1883 |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiSignalCfg interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28582** | N/A | O-TOT-A710-230522/1884 |
| Improper Neutralization of Special Elements | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiWpsCfg | N/A | O-TOT-A710-230522/1885 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in a Command ('Command Injection') | | | interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28583** | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | It is found that there is a command injection vulnerability in the setWiFiWpsStart interface in TOTOlink A7100RU (v7.4cu.2313_b20191024) router, which allows an attacker to execute arbitrary commands through a carefully constructed payload.<br>**CVE ID : CVE-2022-28584** | N/A | O-TOT-A710-230522/1886 |
| **Product: n600r_firmware** | | | | | |
| Improper Neutralization of Special Elements used in a Command ('Command Injection') | 05-May-22 | 9.8 | TOTOLINK N600R v5.3c.5507_B20171031 was discovered to contain a command injection vulnerability via the QUERY_STRING parameter in the "Main" function.<br>**CVE ID : CVE-2022-27411** | N/A | O-TOT-N600-230522/1887 |