

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Jan 2022

Vol. 09 No. 01

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | | | | | |
|---|---------------|-------|---|---|-------------------------|--|--|--|--|--|
| | | | Application | | | | | | | |
| Cisco | Cisco | | | | | | | | | |
| unified_conta | ict_center_ex | press | | | | | | | | |
| Incorrect Resource Transfer Between Spheres | 14-Jan-22 | 8.5 | A vulnerability in the webbased management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) and Cisco Unified Contact Center Domain Manager (Unified CCDM) could allow an authenticated, remote attacker to elevate their privileges to Administrator. This vulnerability is due to the lack of server-side validation of user permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to a vulnerable system. A successful exploit could allow the attacker to create Administrator accounts. With these accounts, the attacker could access and modify telephony and user resources across all the Unified platforms that are associated to the vulnerable Cisco Unified CCMP. To successfully exploit this vulnerability, an attacker would need valid Advanced User credentials. | https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis ory/cisco-sa- ccmp-priv- esc- JzhTFLm4 | A-CIS-UNIF- 210122/1 | | | | | |

3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | | | |
|---|--|------|---|---|-------------------------|--|--|--|
| | | | CVE ID : CVE-2022-20658 | | | | | |
| unified_conta | unified_contact_center_management_portal | | | | | | | |
| Incorrect Resource Transfer Between Spheres | 14-Jan-22 | 8.5 | A vulnerability in the webbased management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) and Cisco Unified Contact Center Domain Manager (Unified CCDM) could allow an authenticated, remote attacker to elevate their privileges to Administrator. This vulnerability is due to the lack of server-side validation of user permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to a vulnerable system. A successful exploit could allow the attacker to create Administrator accounts. With these accounts, the attacker could access and modify telephony and user resources across all the Unified platforms that are associated to the vulnerable Cisco Unified CCMP. To successfully exploit this vulnerability, an attacker would need valid Advanced User credentials. CVE ID: CVE-2022-20658 | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-saccmp-privesc-JzhTFLm4 | A-CIS-UNIF- 210122/2 | | | |
| | Codeigniter | | | | | | | |
| codeigniter Deserializati | | | Codolanitor is an open source | https://githu | A-COD- | | | |
| on of | 04-Jan-22 | 7.5 | CodeIgniter is an open source PHP full-stack web | https://githu b.com/codeig | CODE- | | | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|--|--|-----------------------------|
| Untrusted Data | | | framework. Deserialization of Untrusted Data was found in the `old()` function in CodeIgniter4. Remote attackers may inject autoloadable arbitrary objects with this vulnerability, and possibly execute existing PHP code on the server. We are aware of a working exploit, which can lead to SQL injection. Users are advised to upgrade to v4.1.6 or later. Users unable to upgrade as advised to not use the `old()` function and form_helper nor `RedirectResponse::withInput()` and `redirect()->withInput()`. | niter4/CodeI gniter4/com mit/ce95ed5 765256e2f09 f3513e7d427 90e0d6948f5, https://githu b.com/codeig niter4/CodeI gniter4/secur ity/advisories /GHSA-w6jr- wj64-mc9x | 210122/3 |
| convos | | | | | |
| convos | | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 04-Jan-22 | 3.5 | Convos is an open source multi-user chat that runs in a web browser. Characters starting with "https://" in the chat window create an <a> tag. Stored XSS vulnerability using onfocus and autofocus occurs because escaping exists for "<" or ">" but escaping for double quotes does not exist. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible. CVE ID: CVE-2022-21649 | https://githu b.com/convo s- chat/convos/ security/advi sories/GHSA- xmpj-xwm3- vww7, https://githu b.com/convo s- chat/convos/ commit/86b2 193de375005 ba71d9dd538 43562c6ac18 47c, https://www. | A-CON- CONV- 210122/4 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 3 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|---|---|-----------------------------|
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 04-Jan-22 | 3.5 | Convos is an open source multi-user chat that runs in a web browser. You can't use SVG extension in Convos' chat window, but you can upload a file with an .html extension. By uploading an SVG file with an html extension the upload filter can be bypassed. This causes Stored XSS. Also, after uploading a file the XSS attack is triggered upon a user viewing the file. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible. CVE ID: CVE-2022-21650 | huntr.dev/bo unties/4532a 0ac-4e7c- 4fcf-9fe3- 630e132325c 0/ https://githu b.com/convo s- chat/convos/ security/advi sories/GHSA- mm2v-4v7g- m695, https://githu b.com/convo s- chat/convos/ commit/5c0a 1ec9a2c147b c3b63fd5a48 da5f32e18fe5 df, https://www. huntr.dev/bo unties/ae424 798-de01- | A-CON- CONV- 210122/5 |
| | | | | 4972-b73b- 2db674f8236 8/ | |
| daybydaycrm | | | | | |
| daybyday | | | | | |
| Insufficient Session Expiration | 13-Jan-22 | 5.5 | In DayByDay CRM, versions 2.2.0 through 2.2.1 (latest) 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 | N/A | A-DAY- DAYB- 210122/6 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|--|---|-----------------------------|
| daybyday_crn | 1 | | still have access to the application even after the password was changed. CVE ID: CVE-2022-22113 | | |
| day by day_cri | ' | | In Daybyday CRM, versions | | |
| Missing Authorizatio n | 05-Jan-22 | 4 | 2.0.0 through 2.2.0 are vulnerable to Missing Authorization. An attacker that has the lowest privileges account (employee type user), can view the appointments of all users in the system including administrators. However, this type of user is not authorized to view the calendar at all. | https://githu b.com/Bottel et/Daybyday CRM/commit /a0392f4a4a 14e1e3fedaf6 817aefce69b 6bd661b | A-DAY- DAYB- 210122/7 |
| | | | CVE ID : CVE-2022-22107 | | |
| Missing Authorizatio n | 05-Jan-22 | 4 | In Daybyday CRM, versions 2.0.0 through 2.2.0 are vulnerable to Missing Authorization. An attacker that has the lowest privileges account (employee type user), can view the absences of all users in the system including administrators. This type of user is not authorized to view this kind of information. CVE ID: CVE-2022-22108 | https://githu b.com/Bottel et/Daybyday CRM/commit /fe842ea5ede 237443f1f45 a99aeb83913 3115d8b | A-DAY- DAYB- 210122/8 |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 05-Jan-22 | 3.5 | In Daybyday CRM, version 2.2.0 is vulnerable to Stored Cross-Site Scripting (XSS) vulnerability that allows low privileged application users to store malicious scripts in the title field of new tasks. These scripts are executed in | https://githu b.com/Bottel et/Daybyday CRM/commit /002dc75f40 0cf307bd00b 71a5a93f1e2 6e52cee2 | A-DAY- DAYB- 210122/9 |
| CVSS Scoring Sca | ile 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|---|------------------------------|
| | | | a victim's browser when they open the "/tasks" page to view all the tasks. | | |
| | | | CVE ID : CVE-2022-22109 | | |
| Weak Password Requirement s | 05-Jan-22 | 4 | In Daybyday CRM, versions 1.1 through 2.2.0 enforce weak password requirements in the user update functionality. A user with privileges to update his password could change it to a weak password, such as those with a length of a single character. This may allow an attacker to brute-force users' passwords with minimal to no computational effort. | https://githu b.com/Bottel et/Daybyday CRM/commit /a0392f4a4a 14e1e3fedaf6 817aefce69b 6bd661b | A-DAY- DAYB- 210122/10 |
| | | | CVE ID : CVE-2022-22110 | | |
| Missing Authorizatio n | 05-Jan-22 | 6.5 | In DayByDay CRM, version 2.2.0 is vulnerable to missing authorization. Any application user in the application who has update user permission enabled is able to change the password of other users, including the administrator's. This allows the attacker to gain access to the highest privileged user in the application. CVE ID: CVE-2022-22111 | https://githu b.com/Bottel et/Daybyday CRM/commit /fe842ea5ede 237443f1f45 a99aeb83913 3115d8b | A-DAY- DAYB- 210122/11 |
| digitalbazaar | | | | | |
| forge | | | | | |
| URL Redirection to Untrusted Site ('Open Redirect') | 06-Jan-22 | 5.8 | forge is vulnerable to URL Redirection to Untrusted Site CVE ID : CVE-2022-0122 | https://githu b.com/digital bazaar/forge /commit/db8 016c805371e | A-DIG- FORG- 210122/12 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 6 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|------------------------------|
| | | | | 72b06d8e2ed fe0ace0df934 a5e, https://huntr .dev/bounties /41852c50- 3c6d-4703- 8c55- 4db27164a4a e | |
| discourse | | | | | |
| discourse | | | | | |
| Exposure of Sensitive Information to an Unauthorize d Actor | 05-Jan-22 | 4 | Discourse is an open source platform for community discussion. In affected versions when composing a message from topic the composer user suggestions reveals whisper participants. The issue has been patched in stable version 2.7.13 and beta version 2.8.0.beta11. There is no workaround for this issue and users are advised to upgrade. CVE ID: CVE-2022-21642 | https://githu b.com/discou rse/discourse /commit/702 685b6a06ae4 5a544fc7020 27f1e4573d9 4aaa, https://githu b.com/discou rse/discourse /security/adv isories/GHSA -mx3h-vc7w- r9c6 | A-DIS-DISC- 210122/13 |
| Dolibarr | | | | | |
| dolibarr | | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 02-Jan-22 | 3.5 | admin/limits.php in Dolibarr 7.0.2 allows HTML injection, as demonstrated by the MAIN_MAX_DECIMALS_TOT parameter. CVE ID: CVE-2022-22293 | N/A | A-DOL- DOLI- 210122/14 |
| fit2cloud | | | | | |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|------------------------------|
| halo | | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 13-Jan-22 | 3.5 | In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the article title. An authenticated attacker can inject arbitrary javascript code that will execute on a victim's server. CVE ID: CVE-2022-22123 | N/A | A-FIT- HALO- 210122/15 |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 13-Jan-22 | 3.5 | In Halo, versions v1.0.0 to v1.4.17 (latest) are vulnerable to Stored Cross-Site Scripting (XSS) in the profile image. An authenticated attacker can upload a carefully crafted SVG file that will trigger arbitrary javascript to run on a victim's browser. CVE ID: CVE-2022-22124 | N/A | A-FIT- HALO- 210122/16 |
| framasoft | | | | | |
| peertube | | | | | |
| Server-Side Request Forgery (SSRF) | 10-Jan-22 | 5 | peertube is vulnerable to Server-Side Request Forgery (SSRF) CVE ID: CVE-2022-0132 | https://githu b.com/choco bozzz/peertu be/commit/7 b54a81cccf6b 4c12269e9d6 897d608b1a9 9537a, https://huntr .dev/bounties /77ec5308- 5561-4664- af21- d780df2d1e4 b | A-FRA- PEER- 210122/17 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|----------------|------|---|--|------------------------------|
| Improper Access Control | 10-Jan-22 | 5 | peertube is vulnerable to Improper Access Control CVE ID: CVE-2022-0133 | https://huntr .dev/bounties /80aabdc1- 89fe-47b8- 87ca- 9d68107fc0b 4, https://githu b.com/choco bozzz/peertu be/commit/7 95212f7acc6 90c88c86d0f ab8772f6564 d59cb8 | A-FRA- PEER- 210122/18 |
| hoppscotch | | | | | |
| hoppscotch | | | | | |
| Exposure of Sensitive Information to an Unauthorize d Actor | 06-Jan-22 | 6 | hoppscotch is vulnerable to Exposure of Sensitive Information to an Unauthorized Actor CVE ID: CVE-2022-0121 | https://huntr .dev/bounties /b70a6191- 8226-4ac6- b817- cae7332a68e e, https://githu b.com/hopps cotch/commit /86ef1a4e14 3ea5bb0c7b3 09574127cc3 9d4faa74 | A-HOP- HOPP- 210122/19 |
| ivanti | | | | | |
| workspace_co | ontrol | | | | |
| Insecure Storage of Sensitive Information | 10-Jan-22 | 2.1 | A insecure storage of sensitive information vulnerability exists in Ivanti Workspace Control <2021.2 (10.7.30.0) that could allow | https://foru ms.ivanti.com /s/article/A- locally- authenticated | A-IVA- WORK- 210122/20 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 9 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|----------------|------|--|---|--------------------------|
| | | | an attacker with locally authenticated low privileges to obtain key information due to an unspecified attack vector. CVE ID: CVE-2022-21823 | -user-with- low- privileges- can-obtain- key- information- due-to-an- unspecified- attack- vector?langua ge=en_US | |
| libexpat_proj | ect | | | | |
| libexpat | | | | | |
| Integer Overflow or Wraparound | 10-Jan-22 | 7.5 | addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. CVE ID: CVE-2022-22822 | https://githu b.com/libexp at/libexpat/p ull/539 | A-LIB-LIBE- 210122/21 |
| Integer Overflow or Wraparound | 10-Jan-22 | 7.5 | build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. CVE ID: CVE-2022-22823 | N/A | A-LIB-LIBE- 210122/22 |
| Integer Overflow or Wraparound | 10-Jan-22 | 7.5 | defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. CVE ID: CVE-2022-22824 | https://githu b.com/libexp at/libexpat/p ull/539 | A-LIB-LIBE- 210122/23 |
| Integer Overflow or Wraparound | 10-Jan-22 | 6.8 | lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. CVE ID: CVE-2022-22825 | N/A | A-LIB-LIBE- 210122/24 |
| Integer Overflow or Wraparound | 10-Jan-22 | 6.8 | nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. CVE ID: CVE-2022-22826 | N/A | A-LIB-LIBE- 210122/25 |
| Integer Overflow or Wraparound | 10-Jan-22 | 6.8 | storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | N/A | A-LIB-LIBE- 210122/26 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|--------------------------|
| | | | CVE ID : CVE-2022-22827 | | |
| Lighttpd | | | | | |
| lighttpd | | | | | |
| Out-of- bounds Write | 06-Jan-22 | 4.3 | In lighttpd 1.4.46 through 1.4.63, the mod_extforward_Forwarded function of the mod_extforward plugin has a stack-based buffer overflow (4 bytes representing -1), as demonstrated by remote denial of service (daemon crash) in a non-default configuration. The non-default configuration requires handling of the Forwarded header in a somewhat unusual manner. Also, a 32-bit system is much more likely to be affected than a 64-bit system. CVE ID: CVE-2022-22707 | https://redmi ne.lighttpd.ne t/issues/313 4 | A-LIG-LIGH- 210122/27 |
| livehelpercha | at | | | | |
| live_helper_c | hat | | | | |
| Generation of Error Message Containing Sensitive Information | 04-Jan-22 | 5 | livehelperchat is vulnerable to Generation of Error Message Containing Sensitive Information CVE ID: CVE-2022-0083 | https://huntr .dev/bounties /4c477440- 3b03-42eb- a6e2- a31b5509073 6, https://githu b.com/livehel perchat/liveh elperchat/co mmit/fbed87 28be59040a7 218610e72f6 | A-LIV-LIVE- 210122/28 |

0-1

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|----------------|------|--|---|------------------------------|
| | | | | eceb5f8bc152 | |
| Microsoft | | | | | |
| 365_apps | | | | | |
| N/A | 11-Jan-22 | 9.3 | Microsoft Excel Remote Code Execution Vulnerability. CVE ID: CVE-2022-21841 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21841 | A-MIC-365 210122/29 |
| excel | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 6.8 | Microsoft Office Remote Code Execution Vulnerability. CVE ID: CVE-2022-21840 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21840 | A-MIC- EXCE- 210122/30 |
| exchange_ser | ver | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 8.3 | Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21855, CVE-2022-21969. CVE ID: CVE-2022-21846 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21846 | A-MIC- EXCH- 210122/31 |
| N/A | 11-Jan-22 | 7.7 | Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21846, CVE-2022-21969. CVE ID: CVE-2022-21855 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21855 | A-MIC- EXCH- 210122/32 |
| office | | | | | |
| Improper Control of Generation of Code | 11-Jan-22 | 6.8 | Microsoft Office Remote Code Execution Vulnerability. CVE ID : CVE-2022-21840 | https://porta l.msrc.micros oft.com/en- US/security- | A-MIC-OFFI- 210122/33 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|--|---|------------------------------|
| ('Code Injection') | | | | guidance/adv isory/CVE- 2022-21840 | |
| N/A | 11-Jan-22 | 9.3 | Microsoft Excel Remote Code Execution Vulnerability. CVE ID: CVE-2022-21841 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21841 | A-MIC-OFFI- 210122/34 |
| office_online_ | server | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 6.8 | Microsoft Office Remote Code Execution Vulnerability. CVE ID: CVE-2022-21840 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21840 | A-MIC-OFFI- 210122/35 |
| office_web_ap | ps | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 6.8 | Microsoft Office Remote Code Execution Vulnerability. CVE ID: CVE-2022-21840 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21840 | A-MIC-OFFI- 210122/36 |
| sharepoint_ei | nterprise_ser | ver | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 6.8 | Microsoft Office Remote Code Execution Vulnerability. CVE ID: CVE-2022-21840 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21840 | A-MIC- SHAR- 210122/37 |
| Improper Control of Generation of Code | 11-Jan-22 | 6.8 | Microsoft Word Remote Code Execution Vulnerability. CVE ID: CVE-2022-21842 | https://porta l.msrc.micros oft.com/en- US/security- | A-MIC- SHAR- 210122/38 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|--|---|------------------------------|
| ('Code Injection') | | | | guidance/adv isory/CVE- 2022-21842 | |
| sharepoint_fo | oundation | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 9 | Microsoft SharePoint Server Remote Code Execution Vulnerability. CVE ID: CVE-2022-21837 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21837 | A-MIC- SHAR- 210122/39 |
| sharepoint_so | erver | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 9 | Microsoft SharePoint Server Remote Code Execution Vulnerability. CVE ID: CVE-2022-21837 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21837 | A-MIC- SHAR- 210122/40 |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 6.8 | Microsoft Office Remote Code Execution Vulnerability. CVE ID: CVE-2022-21840 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21840 | A-MIC- SHAR- 210122/41 |
| word | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 11-Jan-22 | 6.8 | Microsoft Word Remote Code Execution Vulnerability. CVE ID: CVE-2022-21842 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21842 | A-MIC- WORD- 210122/42 |
| mruby | <u> </u> | | | | |
| mruby | | | | | |
| Heap-based Buffer | 02-Jan-22 | 7.5 | mruby is vulnerable to Heap- | https://huntr .dev/bounties | A-MRU- MRUB- |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|--|---|------------------------------|
| Overflow | | | based Buffer Overflow CVE ID: CVE-2022-0080 | /59a70392- 4864-4ce3- 8e35- 6ac2111d1e2 e, https://githu b.com/mruby /mruby/com mit/28ccc66 4e5dcd3f9d5 | 210122/43 |
| | | | | 5173e9afde7 7c4705a9ab6 | |
| nette | | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 04-Jan-22 | 4.3 | Latte is an open source template engine for PHP. Versions since 2.8.0 Latte has included a template sandbox and in affected versions it has been found that a sandbox escape exists allowing for injection into web pages generated from Latte. This may lead to XSS attacks. The issue is fixed in the versions 2.8.8, 2.9.6 and 2.10.8. Users unable to upgrade should not accept template input from untrusted sources. CVE ID: CVE-2022-21648 | https://githu b.com/nette/l atte/commit/ 9e1b4f7d70f 7a9c3fa6753f fa7d7e450a3 d4abb0, https://githu b.com/nette/l atte/security /advisories/G HSA-36m2- 8rhx-f36j | A-NET- LATT- 210122/44 |
| phoronix-med | dia | | | | |
| phoronix_test | t_suite | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site | 10-Jan-22 | 3.5 | phoronix-test-suite is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CVE ID: CVE-2022-0157 | https://huntr .dev/bounties /2c0fe81b- 0977-4e1e- b5d8- 7646c9a7ebb d, | A-PHO- PHOR- 210122/45 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 15 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|--|------------------------------|
| Scripting') | | | | https://githu b.com/phoro nix-test- suite/phoroni x-test- suite/commit /56fd0a3b69f b33c1c90a60 17ed735889a aa59486 | |
| rangerstudio | | | | | |
| directus | | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 10-Jan-22 | 3.5 | In Directus, versions 9.0.0- alpha.4 through 9.4.1 are vulnerable to stored Cross- Site Scripting (XSS) vulnerability via SVG file upload in media upload functionality. A low privileged attacker can inject arbitrary javascript code which will be executed in a victim's browser when they open the image URL. CVE ID: CVE-2022-22116 | https://githu b.com/direct us/directus/c ommit/ec86d 5412d45136 915d9b622b 4a890dd2693 2b10 | A-RAN- DIRE- 210122/46 |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 10-Jan-22 | 3.5 | In Directus, versions 9.0.0-alpha.4 through 9.4.1 allow unrestricted file upload of .html files in the media upload functionality, which leads to Cross-Site Scripting vulnerability. A low privileged attacker can upload a crafted HTML file as a profile avatar, and when an admin or another user opens it, the XSS payload gets triggered. CVE ID: CVE-2022-22117 | https://githu b.com/direct us/directus/c ommit/ec86d 5412d45136 915d9b622b 4a890dd2693 2b10 | A-RAN- DIRE- 210122/47 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Shopware is an open source e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible. CVE ID: CVE-2022-21651 Shopware is an open source e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible. CVE ID: CVE-2022-21651 Shopware is an open source e-commerce software platform. In affected versions shopware would not invalidate a user session in the event of a password change. With version 5.7.7 the session validation was DS-Jan-22 Shopware is an open source e-commerce software platform. In affected versions shopware.co m/en/shopw are-5- en/securityu pdates/security-update-01- to-10- t | Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|---|--------------|------|---|---|-----------|
| Shopware is an open source e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible. CVE ID: CVE-2022-21651 Shopware is an open source e-commerce software platform. In affected we to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible. CVE ID: CVE-2022-21651 Shopware is an open source e-commerce software platform. In affected versions shopware would not invalidate a user session in the event of a password change. With version 5.7.7 the session validation was adjusted, so that sessions created prior to the latest password change of a customer account can't be used to login with said account. This also means, that https://githu b.com/shopw are/shopware e/commit/a9 0046c765s.57 a46c4399dce 17bd174253c 32886, https://githu b.com/shopw are/shopware e/security/ods visories/GHS and the plate of th | Shopware | | | | | |
| Shopware is an open source e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible. CVE ID: CVE-2022-21651 Shopware is an open source e-commerce software platform. In affected wersions shopware would not invalidate a user session in the event of a password change of a customer account can't be used to login with said account. This also means, that b.com/shopw are/shopwar e/commit/a9 0046c765c57 a46c4399dce 17bd174253c 32886, https://githu b.com/shopw are/shopwar e/security/ad visories/GHS A-SHO-SHO-SHOP-210122/48 A-SHO-SHOP-210122/48 Brown are/shopwar e/security/updates | shopware | | | | | |
| e-commerce software platform. In affected versions shopware.co m/en/shopw are-5- invalidate a user session in the event of a password change. With version 5.7.7 the session validation was adjusted, so that sessions created prior to the latest password change of a customer account can't be used to login with said account. This also means, that shopware.co m/en/shopw are-5- en/securityu pdates/securi ty-update-01- SHOP- 210122/49 A-SHO-SHOP- 210122/49 | URL Redirection to Untrusted Site ('Open Redirect') | 05-Jan-22 | 5.8 | e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible. CVE ID: CVE-2022-21651 | b.com/shopw are/shopwar e/commit/a9 0046c765c57 a46c4399dce 17bd174253c 32886, https://githu b.com/shopw are/shopwar e/security/ad visories/GHS A-c53v-qmrx- 93hg, https://docs. shopware.co m/en/shopw are-5- en/securityu pdates/securi ty-update-01- 2022 | SHOP- |
| | Insufficient Session Expiration | 05-Jan-22 | 5.5 | e-commerce software platform. In affected versions shopware would not invalidate a user session in the event of a password change. With version 5.7.7 the session validation was adjusted, so that sessions created prior to the latest password change of a customer account can't be used to login with said account. This also means, that | shopware.co m/en/shopw are-5- en/securityu pdates/securi ty-update-01- 2022, https://githu b.com/shopw are/shopwar e/security/ad visories/GHS A-p523-jrph- | SHOP- |
| CVSS Scoring Scale | 0) (00.0 | | | | | |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|--|--|------------------------------|
| | | | existing sessions for a given customer account are automatically considered invalid. There is no workaround for this issue. CVE ID: CVE-2022-21652 | https://githu b.com/shopw are/shopwar e/commit/47 ebd126a94f4 b019b6fde64 c0df3d18d74 ef7d0 | |
| showdoc | | | | | |
| showdoc | | | | | |
| Generation of Error Message Containing Sensitive Information | 03-Jan-22 | 5 | showdoc is vulnerable to Generation of Error Message Containing Sensitive Information CVE ID: CVE-2022-0079 | https://huntr .dev/bounties /b37f0e26- 355a-4d50- 8495- a567c10828e e, https://githu b.com/star7t h/showdoc/c ommit/e43df 0a190f68aefa 272507d3bd 54475f566c1 db | A-SHO- SHOW- 210122/50 |
| sismics | | | | | |
| teedy | | | | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 10-Jan-22 | 4.3 | In Teedy, versions v1.5 through v1.9 are vulnerable to Reflected Cross-Site Scripting (XSS). The "search term" search functionality is not sufficiently sanitized while displaying the results of the search, which can be leveraged to inject arbitrary scripts. These scripts are executed in a victim's browser when they enter the | https://githu b.com/sismic s/docs/comm it/49512295 76d6892dc58 ab8c572e736 39ca82d80c | A-SIS-TEED- 210122/51 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|---|--------------------------|
| | | | crafted URL. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account Takeover of the administrator, by an unauthenticated attacker. CVE ID: CVE-2022-22114 | | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 10-Jan-22 | 3.5 | In Teedy, versions v1.5 through v1.9 are vulnerable to Stored Cross-Site Scripting (XSS) in the name of a created Tag. Since the Tag name is not being sanitized properly in the edit tag page, a low privileged attacker can store malicious scripts in the name of the Tag. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account Takeover of the administrator, and privileges escalation. CVE ID: CVE-2022-22115 | https://githu b.com/sismic s/docs/comm it/49512295 76d6892dc58 ab8c572e736 39ca82d80c | A-SIS-TEED- 210122/52 |
| snipeitapp | | | | | |
| snipe-it | | | | | |
| Incorrect Default Permissions | 12-Jan-22 | 4.9 | snipe-it is vulnerable to Improper Access Control CVE ID : CVE-2022-0179 | https://huntr .dev/bounties /efdf2ead- f9d1-4767- 9f02- d11f762d15e 7, | A-SNI-SNIP- 210122/53 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|---------------|------|---|---|------------------------------|
| | | | | https://githu b.com/snipe/ snipe- it/commit/cf 14a0222c674 72086cd08b2 155f045edaf7 5f2e | |
| soketi_projec | t | | | | |
| soketi | | | | | |
| Improper Handling of Exceptional Conditions | 10-Jan-22 | 5 | webSockets server. There is an unhandled case when reading POST requests which results in the server crashing if it could not read the body of a request. In the event that a POST request is sent to any endpoint of the server with an empty body, even unauthenticated with the Pusher Protocol, it will crash the server. All users that run the server are affected by this vulnerability and it's highly recommended to upgrade to the latest patch. There are no workarounds for this issue. CVE ID: CVE-2022-21667 | https://githu b.com/soketi /soketi/secur ity/advisories /GHSA-86ch- 6w7v-v6xf, https://githu b.com/soketi /soketi/com mit/4b12efef 9c31117c36a 0a0f1c3aa32 114e86364b | A-SOK- SOKE- 210122/54 |
| transloadit | | | | | |
| ирру | | | | | |
| Server-Side Request Forgery (SSRF) | 04-Jan-22 | 7.5 | uppy is vulnerable to Server-Side Request Forgery (SSRF) CVE ID: CVE-2022-0086 | https://githu b.com/transl oadit/uppy/c ommit/fc137 e30a2a3102e b191141f280 d5de20dacdf 8f, | A-TRA- UPPY- 210122/55 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|------------------------------|
| typelevel | | | | https://huntr .dev/bounties /c1c03ef6- 3f18-4976- a9ad- 08c25127912 2 | |
| jawn | | | | | |
| Inadequate Encryption Strength | 05-Jan-22 | 5 | Jawn is an open source JSON parser. Extenders of the 'org.typelevel.jawn.SimpleFac ade' and 'org.typelevel.jawn.MutableF acade' who don't override 'objectContext()' are vulnerable to a hash collision attack which may result in a denial of service. Most applications do not implement these traits directly, but inherit from a library. 'jawn-parser-1.3.1' fixes this issue and users are advised to upgrade. For users unable to upgrade override 'objectContext()' to use a collision-safe collection. | https://githu b.com/typele vel/jawn/pull /390, https://githu b.com/typele vel/jawn/sec urity/advisor ies/GHSA- vc89-hccf- rq55 | A-TYP- JAWN- 210122/56 |
| | | | CVE ID : CVE-2022-21653 | | |
| usoc_project usoc | | | | | |
| Improper | | | USOC is an open source CMS | https://githu | |
| Neutralizatio n of Special Elements used in an SQL Command ('SQL CVSS Scoring Sca | 04-Jan-22 | 7.5 | with a focus on simplicity. In affected versions USOC allows for SQL injection via register.php. In particular usernames, email addresses, and passwords provided by the user were not sanitized | b.com/Aaron- Junker/USOC /commit/21e 8bfd7a9ab0b 7f9344a7a3a 7c32a7cdd5a 0b69, | A-USO- USOC- 210122/57 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|------------------------------|
| Injection') | | | and were used directly to construct a sql statement. Users are advised to upgrade as soon as possible. There are not workarounds for this issue. CVE ID: CVE-2022-21643 | https://githu b.com/Aaron- Junker/USOC /security/adv isories/GHSA -fjp4-phjh- jgmc | |
| Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection') | 04-Jan-22 | 6.5 | USOC is an open source CMS with a focus on simplicity. In affected versions USOC allows for SQL injection via usersearch.php. In search terms provided by the user were not sanitized and were used directly to construct a sql statement. The only users permitted to search are site admins. Users are advised to upgrade as soon as possible. There are not workarounds for this issue. CVE ID: CVE-2022-21644 | https://githu b.com/Aaron- Junker/USOC /security/adv isories/GHSA -89jg-6fr3- 9q4h, https://githu b.com/Aaron- Junker/USOC /commit/062 17c66c8f9b1 14726b2163 3eabcd88ac9 034aa | A-USO- USOC- 210122/58 |
| VIM | | | | | |
| VIIII | | | | https://githu | |
| Out-of- bounds Read | 06-Jan-22 | 6.8 | vim is vulnerable to Out-of- bounds Read CVE ID : CVE-2022-0128 | b.com/vim/vi m/commit/d 3a117814d6a cbf0dca3eff1a 7626843b9b 3734a, https://huntr .dev/bounties /63f51299- 008a-4112- b85b- 1e904aadd4b a | A-VIM-VIM- 210122/59 |

| | | Description & CVE ID | Patch | NCIIPC ID |
|-----------|-----------|--|---|---|
| 10-Jan-22 | 4.3 | vim is vulnerable to Use After Free CVE ID : CVE-2022-0156 | https://githu b.com/vim/vi m/commit/9f 1a39a5d1cd7 989ada2d1cb 32f97d84360 e050f, https://huntr .dev/bounties /47dded34- 3767-4725- 8c7c- 9dcb68c70b3 6 | A-VIM-VIM- 210122/60 |
| 10-Jan-22 | 4.3 | vim is vulnerable to Heap- based Buffer Overflow CVE ID : CVE-2022-0158 | https://huntr .dev/bounties /ac5d7005- 07c6-4a0a- b251- ba9cdbf6738 b, https://githu b.com/vim/vi m/commit/5f 25c3855071b d7e26255c68 bf458b1b5cf9 2f39 | A-VIM-VIM- 210122/61 |
| | | | | |
| 1 | | | I | |
| 06-Jan-22 | 5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain | https://githu b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA- 6676-cqfm- gw84, https://word | A-WOR- WORD- 210122/62 |
| | 10-Jan-22 | 10-Jan-22 4.3 06-Jan-22 5 | 10-Jan-22 4.3 vim is vulnerable to Heapbased Buffer Overflow CVE ID: CVE-2022-0158 WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain | 10-Jan-22 4.3 vim is vulnerable to Use After Free CVE ID: CVE-2022-0156 vim is vulnerable to Heap-based Buffer Overflow CVE ID: CVE-2022-0158 vim is vulnerable to Heap-based Buffer Overflow CVE ID: CVE-2022-0158 wim is vulnerable to Heap-based Buffer Overflow CVE ID: CVE-2022-0158 WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain b.com/vim/vi m/commit/9f 1a39a5d1cd7 989ada2d1cb 32f97d84360 e050f, https://huntr .dev/bounties /47dded34-3767-4725-8c7c-9dcb68c70b3 6 https://huntr .dev/bounties /47dded34-3767-4725-8c7c-9dcb68c70b3 6 https://huntr .dev/bounties /47dded34-3767-4725-8c7c-9dcb68c70b3 6 https://jgithu b.com/vim/vi m/commit/9f 1a39a5d1cd7 989ada2d1cb 32f97d84360 e050f, https://huntr .dev/bounties /47dded34-3767-4725-8c7c-9dcb68c70b3 6 https://huntr .dev/bounties /47dded34-3767-4725-8c7c-9dcb68c70b3 6 https://jgithu b.com/vim/vi m/commit/9f 1a39a5d1cd7 989ada2d1cb 32f97d84360 e050f, https://huntr .dev/bounties /47dded34-3767-4725-8c7c-9dcb68c70b3 6 https://jeithu b.com/vim/vi m/commit/5f 25c3855071b d7e26255c68 bf458b1b5cf9 2f39 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|---|------------------------------|
| | | | way. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this vulnerability. CVE ID: CVE-2022-21661 | press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, https://githu b.com/Word Press/wordp ress- develop/com mit/17efac8c 8ec64555eff5 cf51a3eff81e 06317214 | |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') | 06-Jan-22 | 3.5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Low-privileged authenticated users (like author) in WordPress core are able to execute JavaScript/perform stored XSS attack, which can affect high-privileged users. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. | https://word press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, https://githu b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA- 699q-3hj9- 889w | A-WOR- WORD- 210122/63 |
| Improper Neutralizatio n of Special Elements in Output Used | 06-Jan-22 | 6.5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a | https://word press.org/ne ws/2022/01/ wordpress-5- 8-3-security- | A-WOR- WORD- 210122/64 |

0-1

2-3 3-4 4-5 5-6

| multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. CVE ID : CVE-2022-21663 WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. CVE ID : CVE-2022-21664 Hardware mediatek awus036nh N/A 04-Jan-22 3.3 In Bluetooth, there is a https://corp. H-MED- | Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID | | |
|---|--|--------------|------|---|--|-----------|--|--|
| WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. CVE ID : CVE-2022-21664 CVE ID | Downstream Component | | | Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. | https://githu b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA- jmmq-m8p8- | | | |
| mediatek awus036nh N/A 04-Jan-22 3.3 In Bluetooth, there is a https://corp. H-MED- | Neutralizatio n of Special Elements used in an SQL Command ('SQL | 06-Jan-22 | 6.5 | open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. | press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, https://githu b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA-jp3p- | WORD- | | |
| awus036nh N/A 04-Jan-22 3.3 In Bluetooth, there is a https://corp. H-MED- | Hardware | | | | | | | |
| N/A 04-Jan-22 3.3 In Bluetooth, there is a https://corp. H-MED- | | | | | | | | |
| N/A | awus036nh | | | I. Di aradi di | hu // | II MED | | |
| | , | | | possible application crash | mediatek.com | AWUS- | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|--------------|------|---|--|------------------------------|
| | | | due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | /product- security- bulletin/Janu ary-2022 | 210122/66 |
| mt6580 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT65- 210122/67 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT65- 210122/68 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a | https://corp. | H-MED- |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|------------------------------|
| | | | possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | mediatek.com /product- security- bulletin/Janu ary-2022 | MT65- 210122/69 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT65- 210122/70 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT65- 210122/71 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | | | | |
|---|--------------|------|--|--|------------------------------|--|--|--|--|
| | | | ID: ALPS06198608; Issue ID: ALPS06198608. | | | | | | |
| | | | CVE ID : CVE-2022-20023 | | | | | | |
| mt6595 | mt6595 | | | | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT65- 210122/72 | | | | |
| | | | CVE ID : CVE-2022-20019 | | | | | | |
| mt6630 | | | | | | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT66- 210122/73 | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT66- 210122/74 | | | | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 | | | | |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|------------------------------|
| | | | currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT66- 210122/75 |
| mt6735 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/76 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not | https://corp. mediatek.com /product- | H-MED- MT67- 210122/77 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| | | | properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | security- bulletin/Janu ary-2022 | |
|--|---------|-----|--|--|------------------------------|
| | | | CVE ID : CVE-2022-20021 | | |
| | -Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/78 |
| Missing Release of Resource after Effective Lifetime | -Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/79 |

| Memory Buffer Memory Buffer Memory Memo | Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID | | | |
|--|---|--------------|------|---|---|-----------|--|--|--|
| Improper Restriction of Operations within the Bounds of a Memory Buffer N/A 04-Jan-22 3.3 N/A 04-Jan-22 3.3 N/A 04-Jan-22 3.3 N/A 04-Jan-22 3.3 In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620. CVE ID: CVE-2022-20019 In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host connection_req. This could lead to remote denial of service of bluetooth with no additional executity-bulletin/Janu ary-2022 H-MED-MT67-210122/st bulletin/Janu ary-2022 In Bluetooth, there is a possible application crash due to bluetooth does not properly handle aconnection privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote This could lead to remote The MED-MT67-210122/st bulletin/Janu ary-2022 H-MED-MT67-210122/st bulletin/Janu ary-2022 | | | | CVE ID : CVE-2022-20023 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer N/A 04-Jan-22 3.3 Is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote | mt6737 | | | | | | | | |
| N/A 04-Jan-22 3.3 O4-Jan-22 Jan-22 Jan-24 Jan-22 Jan-22 Jan-22 Jan-22 Jan-22 Jan-22 Jan-22 Jan-24 Jan-22 Jan-23 Jan-22 Jan-23 Jan-24 Jan-24 | Restriction of Operations within the Bounds of a Memory | 04-Jan-22 | 2.1 | is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | mediatek.com /product- security- bulletin/Janu | | | | |
| N/A 04-Jan-22 3.3 possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote This could lead to remote possible link disconnection https://corp. mediatek.com /product-security-bulletin/Janu ary-2022 | N/A | 04-Jan-22 | 3.3 | possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | mediatek.com /product- security- bulletin/Janu | | | | |
| denial of service of bluetooth with no additional execution | N/A | 04-Jan-22 | 3.3 | possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth | mediatek.com /product- security- bulletin/Janu | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|------------------------------|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/83 |
| mt6739 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/84 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/85 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|------------------------------|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/86 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/87 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/88 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|--|------------------------------|
| | | | ALPS05943906. | | |
| | | | CVE ID : CVE-2022-20020 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/89 |
| | | | CVE ID : CVE-2022-20021 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/90 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/91 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 34 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|------------------------------|
| | | | bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | | |
| mt6750 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/92 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/93 |
| mt6750s | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with | https://corp. mediatek.com /product- security- bulletin/Janu | H-MED- MT67- 210122/94 |

0-1

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|------------------------------|
| | | | no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | ary-2022 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/95 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/96 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the | https://corp. mediatek.com /product- security- bulletin/Janu | H-MED- MT67- 210122/97 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|------------------------------|
| | | | same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | ary-2022 | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/98 |
| mt6753 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/99 |
| Improper Restriction | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information | https://corp. mediatek.com | H-MED- MT67- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|---------------|------|--|--|-------------------------------|
| of Operations within the Bounds of a Memory Buffer | | | disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | /product- security- bulletin/Janu ary-2022 | 210122/100 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/101 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/102 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| mt6755s | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/106 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/107 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/108 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | | |
| | | | CVE ID : CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/109 |
| | | | CVE ID : CVE-2022-20023 | | |
| mt6757 | | | | | T |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/110 |
| | | | CVE ID : CVE-2022-20012 | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/111 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. | | |
| | | | CVE ID : CVE-2022-20015 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/112 |
| | | | CVE ID : CVE-2022-20018 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/113 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/114 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | | Descriptio | n & CVE | ID | Pa | itch | NCIII | PC ID |
|---|----------------|------|---|--|---|--|-------------------------|-------------------------|-------------------------|-------|
| | | | ALPSO | tation. P 1619851 1619851 | 3; Issue | | | | | |
| | | | CVE II | D : CVE-2 | 2022-20 | 0021 | | | | |
| N/A | 04-Jan-22 | 3.3 | possible due to prope attemposame in terms of the contract with many privile interact exploit ALPSO ALPSO | etooth, to le link do bluetoo rly hand pt from a BD addrould lead of servino addition addition. Pole 19857 D: CVE-2 | isconne th does le a con a host w ess as th ected B d to rem ce of blu onal exe ded. Use atch ID: 8; Issue 8. | ction not nection ith the ne T host. ote netooth cution er led for | media /prodi | ty- n/Janu | H-MEI MT67- 21012 | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not | | media /prodi securi | ty- n/Janu | H-MEI MT67- 21012 | | | |
| mt6757c | | | | | | | | | | |
| Improper Initialization | 04-Jan-22 | 2.1 | there inforn uninit | In kd_camera_hw driver, there is a possible information disclosure due to uninitialized data. This could lead to local information | | media /prodi securi | | H-MEI MT67- 21012 | | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | ary-2022 | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/118 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/119 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/120 |

0-1

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|--|--|-------------------------------|
| | | | with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/121 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/122 |
| mt6757cd | | | | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, there is a possible | https://corp. mediatek.com | H-MED- MT67- |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | /product- security- bulletin/Janu ary-2022 | 210122/123 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/124 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/125 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple | https://corp. mediatek.com /product- security- bulletin/Janu | H-MED- MT67- 210122/126 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | ary-2022 | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/127 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/128 |

6-7 7-8 8-9

CVSS Scoring Scale

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|--|-------------------------------|
| mt6757ch | | | | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/129 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/130 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/131 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash | https://corp. mediatek.com | H-MED- MT67- |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 48 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | /product- security- bulletin/Janu ary-2022 | 210122/132 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/133 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/134 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | ALPS06198608. | | |
| | | | CVE ID : CVE-2022-20023 | | |
| mt6758 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/135 |
| | | | CVE ID : CVE-2022-20019 | | |
| mt6761 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/136 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/137 |

0-1

6-7 7-8

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|--|-------------------------------|
| | | | ALPS05862966. | | |
| | | | CVE ID : CVE-2022-20015 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/138 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/139 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/140 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|--------------|------|---|--|-------------------------------|
| mt6762 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/141 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/142 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/143 |
| Improper Restriction | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information | https://corp. mediatek.com | H-MED- MT67- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| of Operations within the Bounds of a Memory Buffer | | | disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | /product- security- bulletin/Janu ary-2022 | 210122/144 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/145 |
| mt6763 | | | | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/146 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, there is a possible information disclosure due to | https://corp. mediatek.com /product- | H-MED- MT67- 210122/147 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Improper Restriction of Operations within the Bounds of a Memory Buffer N/A | Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|---|--------------|------|---|---|-----------|
| Improper Restriction of Operations within the Bounds of a Memory Buffer N/A 04-Jan-22 N/A 04-Jan-22 3.3 Is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620. CVE ID: CVE-2022-20019 In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 N/A 04-Jan-22 Jn Bluetooth, there is a possible link disconnection mediatek.com MT67- mediatek.com https://corp. mediatek.com /product-security-bulletin/Janu ary-2022 H-MED-MT67- 210122/148 | | | | lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | bulletin/Janu | |
| N/A 04-Jan-22 3.3 04-Jan-22 3.3 Describe application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 In Bluetooth, there is a possible link disconnection N/A 04-Jan-22 Jin Bluetooth, there is a possible link disconnection https://corp. MT67- | Restriction of Operations within the Bounds of a Memory | 04-Jan-22 | 2.1 | is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | mediatek.com /product- security- bulletin/Janu | MT67- |
| N/A 04-Jan-22 3.3 possible link disconnection mediatek.com MT67- | N/A | 04-Jan-22 | 3.3 | possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | mediatek.com /product- security- bulletin/Janu | MT67- |
| | N/A | 04-Jan-22 | 3.3 | possible link disconnection | mediatek.com | MT67- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|---|--|-------------------------------|
| | | | properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | security- bulletin/Janu ary-2022 | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/151 |
| mt6765 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/152 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|--|-------------------------------|
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/153 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/154 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/155 |
| Missing Release of Resource | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a | https://corp. mediatek.com /product- | H-MED- MT67- 210122/156 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 56 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------------|------|---|--|-------------------------------|
| after Effective Lifetime | | | device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | security- bulletin/Janu ary-2022 | |
| mt6768 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/157 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/158 |
| Use of Uninitialized Resource CVSS Scoring Sca | 04-Jan-22 le 0-1 | 2.1 | In seninf driver, there is a possible information disclosure due to uninitialized data. This could | https://corp. mediatek.com /product- security- | H-MED- MT67- 210122/159 |

| Weakness | Publish Date | CVSS | 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: ALPS05863018; Issue ID: ALPS05863018. | bulletin/Janu ary-2022 | |
| | | | CVE ID : CVE-2022-20018 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/160 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/161 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/162 |

0-1

2-3 3-4 4-5 5-6

| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | | |
|---|----------|-----|--|--|-------------------------------|
| | | | CVE ID : CVE-2022-20023 | | |
| mt6769 | | | | | |
| Integer Overflow or Wraparound | 4-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/163 |
| Use of Uninitialized 04 Resource | 4-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/164 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer CVSS Scoring Scale | 4-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/165 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|--------------|------|---|--|-------------------------------|
| | | | needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | | |
| | | | CVE ID : CVE-2022-20019 | | |
| mt6771 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/166 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/167 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/168 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | ALPS05863018. | | |
| | | | CVE ID : CVE-2022-20018 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/169 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/170 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/171 |

0-1

2-3 3-4 4-5 5-6

| | | | Description & CVE ID | Patch | NCIIPC ID |
|--|-----------|-----|---|--|-------------------------------|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/172 |
| mt6779 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/173 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/174 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/175 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/176 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/177 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | ALPS05943906. | | |
| | | | CVE ID : CVE-2022-20020 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/178 |
| | | | CVE ID : CVE-2022-20023 | | |
| mt6781 | , | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/179 |
| | | | In vow driver, there is a | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/180 |

0-1

2-3 3-4 4-5 5-6

6-7 7-8

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|----------------|------|---|--|-------------------------------|
| | | | CVE ID : CVE-2022-20014 | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/181 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/182 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/183 |
| Improper | 04 Ion 22 | 2.1 | In libMtkOmxGsmDec, there | https://corp. | H-MED- |
| Restriction of | 04-Jan-22 | 2.1 | is a possible information disclosure due to an incorrect | mediatek.com /product- | MT67- 210122/184 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Operations within the Bounds of a Memory Buffer | | | bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | security- bulletin/Janu ary-2022 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/185 |
| mt6785 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/186 |
| Concurrent Execution using Shared Resource with CVSS Scoring Sca | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System 2-3 3-4 4-5 5-6 | https://corp. mediatek.com /product- security- bulletin/Janu | H-MED- MT67- 210122/187 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Improper Synchronizat ion ('Race Condition') | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05837742. | ary-2022 | |
| | | | CVE ID : CVE-2022-20013 | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/188 |
| | | | CVE ID : CVE-2022-20014 | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/189 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/190 |

0-1

6-7 7-8

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | ALPS05862986. | | |
| | | | CVE ID : CVE-2022-20016 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/191 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/192 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/193 |

| Weakness | Publish Date | CVSS | D | escriptio | n & CVE | ID | Pa | atch | NCI | IPC ID |
|---|--------------|------|---|--|---|---|--------------------------|-----------------------|-----------------------|--------|
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | | | | media /prod securi | ty- in/Janu | H-ME MT67 21012 | |
| mt6795 | | | | | | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | is a post disclos bounds to local disclos executi User in needed ID: ALF ALPSO! | s check. l inform sure witl ion priv nteractic | formation to an in This con ation no addinges not on is not olditation 7620; Issue. | on acorrect uld lead ditional eeded. m. Patch sue ID: | media /prod securi | ty- in/Janu | H-ME MT67 21012 | |
| mt6797 | | | | | | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | | | media /prod securi | ty- in/Janu | H-ME MT67 21012 | | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| mt6799 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT67- 210122/197 |
| mt6833 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/198 |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/199 |
| Improper | 04-Jan-22 | 4.6 | In vow driver, there is a | https://corp. | H-MED- |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|---|--|-------------------------------|
| Input Validation | | | possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | mediatek.com /product- security- bulletin/Janu ary-2022 | MT68- 210122/200 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/201 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | | H-MED- MT68- 210122/202 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, there is a possible information disclosure due to uninitialized data. This could lead to local information | https://corp. mediatek.com /product- security- bulletin/Janu | H-MED- MT68- 210122/203 |

0-1

6-7 7-8

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | ary-2022 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/204 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/205 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/206 |

0-1

6-7 7-8

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|----------------|------|--|--|-------------------------------|
| | | | User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | | |
| | | | CVE ID : CVE-2022-20023 | | |
| mt6853 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/207 |
| | | | CVE ID : CVE-2022-20012 | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/208 |
| | | | In vow driver, there is a | | |
| Improper Input Validation | nput 04-Jan-22 | | possible memory corruption 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: ALPS05857308; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/209 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | |
|-------------------------------------|----------------|------|---|--|-------------------------------|--|
| | | | ALPS05857308. | | | |
| | | | CVE ID : CVE-2022-20014 | | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/210 | |
| | | | CVE ID : CVE-2022-20015 | | | |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/211 | |
| | | | CVE ID : CVE-2022-20016 | | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/212 | |
| Improper | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there | https://corp. | H-MED- | |
| Restriction | 01 jaii 22 | | is a possible information | mediatek.com | MT68- | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|---|--|-------------------------------|
| of Operations within the Bounds of a Memory Buffer | | | disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | /product- security- bulletin/Janu ary-2022 | 210122/213 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/214 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/215 |
| mt6853t | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption due to an integer overflow. | https://corp. mediatek.com /product- | H-MED- MT68- 210122/216 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. | security- bulletin/Janu ary-2022 | |
| | | | CVE ID : CVE-2022-20012 | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | H-MED- MT68- 210122/217 | |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/218 |
| Improper Initialization | 1 04-lan-// | | In kd_camera_hw driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/219 |

0-1

2-3 3-4 4-5 5-6

| Use of Uninitialized Resource Use of Uninitialized Resource Use of Uninitialized Resource Use of Uninitialized Resource O4-Jan-22 Use of Uninote is not needed for exploitation of privileges needed. User interaction is not needed for exploitation patch ib: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 In semind driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure due to uninitialized attain privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018. CVE ID: CVE-2022-20016 In semind driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure due to uninitialized needed for exploitation. Patch ID: ALPS05863018. CVE ID: CVE-2022-20018 Improper Restriction of Operations within the Bounds of a Memory Buffer User interaction is not needed for exploitation. Patch ID: ALPS059617620. Issue ID: ALPS05917620. Issue ID: ALPS05917620. | Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|---|--------------|------|---|---|-----------|
| Improper Locking Use of Uninitialized Resource Use of Uninitialized Resource Improper Restriction of Operations of Operations of Operations within the Bounds of a Memory Buffer Use of Unimproper Restriction of Operations of Operations within the Bounds of a Memory Buffer Improper Locking In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986. CVE ID: CVE-2022-20016 In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05 | | | | needed for exploitation. Patch ID: ALPS05862966; Issue ID: | | |
| Improper Locking 04-Jan-22 4.6 Use of Uninitialized Resource Improper Restriction of Operations within the Bounds of a Memory Buffer 04-Jan-22 14.6 Use of Uninitialized Resource Improper Restriction of Operations within the Bounds of a Memory Buffer O4-Jan-22 O4-Ja | | | | CVE ID : CVE-2022-20015 | | |
| Use of Uninitialized Resource 04-Jan-22 In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018. CVE ID: CVE-2022-20018 In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620; Issue ID: In seninf driver, there is a possible information disclosure with System emediatek.com /product-security-bulletin/Janu ary-2022 H-MED-MT68-210122/222 H-MED-MT68-210122/222 | | 04-Jan-22 | 4.6 | possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: | mediatek.com /product- security- bulletin/Janu | MT68- |
| Use of Uninitialized Resource 04-Jan-22 2.1 Improper Restriction of Operations within the Bounds of a Memory Buffer 04-Jan-22 04-Jan-22 04-Jan-22 2.1 possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: H-MED-MT68-210122/221 H-MED-MT68-210122/222 H-MED-MT68-210122/2 | | | | CVE ID : CVE-2022-20016 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer O4-Jan-22 D4-Jan-22 Bounds of a Memory Buffer D4-Jan-22 D4-Jan-22 B1- is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: D4-Jan-22 D5-Jan-22 D5-Jan-2 | Uninitialized | 04-Jan-22 | 2.1 | possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | mediatek.com /product- security- bulletin/Janu | MT68- |
| | Restriction of Operations within the Bounds of a Memory | | 2.1 | is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: | mediatek.com /product- security- bulletin/Janu | MT68- |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|--|---|--|-------------------------------|
| | | | CVE ID : CVE-2022-20019 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/223 |
| | | | CVE ID: CVE-2022-20023 | | |
| mt6873 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/224 |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/225 |

6-7 7-8

8-9

CVSS Scoring Scale

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|---|--|-------------------------------|
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/226 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/227 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | | H-MED- MT68- 210122/228 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, there is a possible information disclosure due to uninitialized data. This could | https://corp. mediatek.com /product- security- | H-MED- MT68- 210122/229 |

0-1

2-3 3-4 4-5 5-6

6-7 7-8

| Weakness | Publish Date | CVSS | 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: ALPS05863018; Issue ID: ALPS05863018. | bulletin/Janu ary-2022 | | |
| | | | CVE ID : CVE-2022-20018 | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/230 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/231 | |
| Missing Release of Resource after Effective Lifetime | elease of esource O4-Jan-22 3.3 | | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/232 | |

0-1

2-3 3-4 4-5 5-6

| Use of Uninitialized Resource 04-Jan-22 Improper Restriction of Operations within the Improper Restriction of Operations within the 04-Jan-22 O4-Jan-22 O4-Jan-22 O4-Jan-22 O4-Jan-22 In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds check. This could lead to local information disclosure due to an incorrect bounds dead to local information disclosure due to an incorrect bounds dead to | Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|---|--------------|------|--|---|-----------|
| Integer Overflow or Wraparound Use of Uninitialized Resource Use of Uninitialized Resource Use of Uninitialized Resource Use of Uninitialized Resource O4-Jan-22 O4-Jan-22 | | | | User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | | |
| Integer Overflow or Wraparound 04-Jan-22 Use of Uninitialized Resource Use of Uninitialized Resource O4-Jan-22 Resource 04-Jan-22 Resource O4-Jan-22 Resource D4-Jan-22 Resource D5- Resource D4-Jan-22 Resource D5- Resource D6- Resource D6- Resource D6- Resource D7- Resource Restriction O6- Operations Within the Bounds of a Memory D6- Resource Resulter Restriction Of Operations Within the Bounds of a Memory D6- Resource Restriction Of Operations Within the Resource D6- Resource Restriction Of Operations Within the Resource Restriction Of Operations Within the Resource Restriction Of Operations Within the Resource D6- Resource Restriction Of Operations Within the Resource Resource Restriction Of Operations Within the Resource Restriction Of Operations Within the Resource Resource Restriction Of Operations Within the Resource Resource Restriction Of Operations Within the Resource Resource Resource Resource Resource Resource Restriction Of Operations Within the Resource | mt6875 | | | | | |
| Use of Uninitialized Resource 04-Jan-22 Improper Restriction of Operations within the Bounds of a Memory 04-Jan-22 | Overflow or | 04-Jan-22 | 4.6 | possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | mediatek.com /product- security- bulletin/Janu | |
| Restriction of Operations within the Bounds of a Memory O4-Jan-22 Memory D4-Jan-22 Bounds of a Memory D4-Jan-22 D4-Jan-22 D4-Jan-22 D4-Jan-22 D4-Jan-22 D5-Jan-22 D6-Jan-22 D7-Jan-22 D7- | Uninitialized | 04-Jan-22 | 2.1 | possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | mediatek.com /product- security- bulletin/Janu | |
| | Restriction of Operations within the Bounds of a Memory | 04-Jan-22 | 2.1 | is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. | mediatek.com /product- security- bulletin/Janu | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. | | |
| mt6877 | | | CVE ID : CVE-2022-20019 | | |
| mtoo// | | | In mdp driver, there is a | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/236 |
| | | | CVE ID : CVE-2022-20012 | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/237 |
| | | | CVE ID: CVE-2022-20013 | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/238 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID | | |
|-------------------------------------|----------------|------|---|--|-------------------------------|--|--|
| | | | CVE ID : CVE-2022-20014 | | | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/239 | | |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/240 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/241 | | |
| Improper | 04 I 22 | 2.4 | In libMtkOmxGsmDec, there | https://corp. | H-MED- | | |
| Restriction of | 04-Jan-22 | 2.1 | is a possible information disclosure due to an incorrect | mediatek.com /product- | MT68- 210122/242 | | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 | | |

| Weakness | Publish Date | CVSS | ı | Description | n & CVE | ID | Pa | itch | NCI | IPC ID |
|---|---------------|------|---|---|---|---|-----------------------------|-----------------------------------|----------------------|--------|
| Operations within the Bounds of a Memory Buffer | | | to loca disclos execut User in neede ID: AL ALPSO | Is check. Is inform Sure with tion priv nteraction d for exp PS05917 D: CVE-2 | ation h no add ileges no on is not oloitation 7620; Iss 0. | litional eeded. n. Patch sue ID: | securi bulleti ary-20 | n/Janu | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | possib disclosi bound to loca disclosi execut User in neede ID: AL ALPSO | rcodecdrole informatic informatic with the control of the control | nation to a mis This cou ation h no add ileges no on is not bloitation 3906; Iss 6. | media /prod securi | ty- n/Janu | H-ME MT68 2101 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | packet. This could lead to | | | | media /prod securi | ty- n/Janu | H-ME MT68 2101 | |
| mt6883 | | | | | | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | possib due to | In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local | | | | //corp. tek.com uct- ty- | H-ME MT68 2101 | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. | bulletin/Janu ary-2022 | |
| | | | CVE ID : CVE-2022-20012 | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/246 |
| | | | CVE ID : CVE-2022-20013 | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/247 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/248 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | | Description | on & CVE | ID | Pa | atch | NCI | IPC ID |
|---|---------------|------|---|---|---|----------------------------------|--------------------------|---|-----------------------|--------|
| | | | ID: AL | d for exp PS05862 586296 | 2966; Is | n. Patch sue ID: | | | | |
| | | | CVE II |) : CVE-2 | 2022-20 | 0015 | | | | |
| Improper Locking | 04-Jan-22 | 4.6 | possib due to could l of priv execut User in needed ID: AL | driver, le memo improp ead to lo ilege wi ion priv nteraction for exp PS05862 586298 | ory corr er locking ocal escath Syste ileges non is not oloitatio 2986; Is | uption ng. This alation m eeded. | media /prod securi | ty- in/Janu | H-ME MT68 21012 | |
| | | | |) : CVE-2 | | | | | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | possib disclos uniniti lead to disclos execut User ir needed ID: ALI ALPSO | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | | | | //corp. tek.com uct- ty- in/Janu 022 | H-ME MT68 2101 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | | | media /prod securi | ty- in/Janu | H-ME MT68 2101 | | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|----------------|------|--|--|-------------------------------|
| mt6885 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/252 |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/253 |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/254 |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, there is a possible information disclosure due to | https://corp. mediatek.com /product- | H-MED- MT68- 210122/255 |
| CVSS Scoring Sca | nle 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862966. | security- bulletin/Janu ary-2022 | |
| | | | CVE ID : CVE-2022-20015 | | |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/256 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/257 |
| Improper Restriction of Operations within the Bounds of a Memory | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/258 |

0-1

| Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|-----------|---|--|--|
| | | User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | | |
| 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/259 |
| 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/260 |
| | | | | |
| Integer Overflow or Wraparound 04-Jan-22 4.6 | | In mdp driver, there is a possible memory corruption 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 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/261 |
| | 04-Jan-22 | 04-Jan-22 3.3 04-Jan-22 4.6 | User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 In mdp driver, there is a possible memory corruption 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: ALPS06198608. CVE ID: CVE-2022-20023 | User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608. CVE ID: CVE-2022-20023 In mdp driver, there is a possible memory corruption 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 local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch local escalation of privilege with no additional execution privileges needed. User interaction is not needed for product-security-bulletin/Janu ary-2022 |

| Weakness | Publish Date | CVSS | ı | Description | n & CVE | ID | Pa | atch | NCI | PC ID |
|--|---------------|------|---|---------------------------------|----------|--------------------------|-----------------------------------|-----------------------|-----------------------|-------|
| | | | ALPSO | tation. P 0583647 0583647 | 8; Issue | | | | | |
| | | | CVE II | D : CVE-2 | 2022-20 | 0012 | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 In vow driver, there is a | | | | tek.com uct- ty- in/Janu | H-ME MT68 21012 | | |
| | | | | | | | | | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for | | | | media /prod securi | ty- in/Janu | H-ME MT68 21012 | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | | | media /prod securi | ty- in/Janu | H-ME MT68 21012 | | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Improper Locking | 04-Jan-22 | 4.6 | User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 In seninf driver, there is a | | H-MED- MT68- 210122/265 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | | | H-MED- MT68- 210122/266 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/267 |
| Missing Release of Resource after | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand | https://corp. mediatek.com /product- security- | H-MED- MT68- 210122/268 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|--|-------------------------------|
| Effective Lifetime | | | packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | bulletin/Janu ary-2022 | |
| mt6891 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/269 |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/270 |
| Improper Input Validation CVSS Scoring Sca | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution 2-3 3-4 4-5 5-6 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/271 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | | |
| | | | In vow driver, there is a | | |
| Improper Locking | 04-Jan-22 | 4.6 | possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. | to improper locking. This ld lead to local escalation privilege with System cution privileges needed. r interaction is not ded for exploitation. Patch ALPS05862986; Issue ID: PS05862986. EID: CVE-2022-20016 | |
| | | | CVE ID: CVE-2022-20016 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/273 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/274 |

0-1

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | ALPS05917620. | | |
| | | | CVE ID : CVE-2022-20019 | | |
| mt6893 | | | | 1 | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/275 |
| | | | CVE ID: CVE-2022-20012 | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/276 |
| | | | | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/277 |
| | | | CVE ID . CVE-2022-20014 | | |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/278 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/279 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT68- 210122/280 |
| Improper Restriction of Operations | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead | https://corp. mediatek.com /product- security- | H-MED- MT68- 210122/281 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | | Descriptio | on & CVE | ID | Pa | itch | NCII | PC ID |
|---|----------------|------|---|---|--|--|---------------------------|-----------------------|-----------------------|-------------|
| within the Bounds of a Memory Buffer | | | disclos execut User in neede ID: AL ALPS0 | Il inform sure wit cion priv nteraction d for exp PS0591 591762 D: CVE-2 | h no add ileges n on is not bloitatio 7620; Is 0. | eeded. n. Patch sue ID: | bulleti ary-20 | n/Janu 22 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 In Bluetooth, there is a | | | media /prodi | ty- n/Janu | H-ME MT68 21012 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | possib due to device packet remot blueto execut User in needed ID: AL ALPSO | | | | media /prodi securi | ty- n/Janu | H-ME MT68 21012 | |
| mt7662t | | | | | | | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple | | | possible application crash due to bluetooth does not properly handle the reception securit | | | | - 22/284 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | ary-2022 | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/285 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/286 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID Patch | | NCIIPC ID |
|--|--------------|------|--|--|-------------------------------|
| mt7663 | | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/287 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/288 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/289 |

0-1

6-7 7-8

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|-----------------|----------------|------|--|--|-------------------------------|
| | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | | |
| mt7668 | | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/290 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT76- 210122/291 |
| Missing | 04-Jan-22 | 3.3 | In Bluetooth, there is a | https://corp. | H-MED- |
| CVSS Scoring Sc | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|--|-------------------------------|
| Release of Resource after Effective Lifetime | | | possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | mediatek.com /product- security- bulletin/Janu ary-2022 | MT76- 210122/292 |
| mt7915 | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT79- 210122/293 |
| mt7920 | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT79- 210122/294 |
| CVSS Scoring Scal | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | | | | |
|---|--------------|------|---|--|-------------------------------|--|--|--|--|
| | | | CVE ID : CVE-2022-20023 | | | | | | |
| mt7921 | mt7921 | | | | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT79- 210122/295 | | | | |
| m+7022 | | | CVE ID : CVE-2022-20023 | | | | | | |
| mt7922 | | | In Direct oath the collection | | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT79- 210122/296 | | | | |
| mt8127 | | | | | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/297 | | | | |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|--------------|------|--|--|-------------------------------|
| | | | exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. | | |
| | | | CVE ID : CVE-2022-20012 | | |
| mt8163 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/298 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/299 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/300 |

| Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--------------|-----------|---|---|---|
| | | This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | | |
| 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/301 |
| | | | | |
| 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/302 |
| 04-Jan-22 | 2.1 | In seninf driver, there is a possible information disclosure due to uninitialized data. This could | https://corp. mediatek.com /product- security- | H-MED- MT81- 210122/303 |
| | 04-Jan-22 | 04-Jan-22 3.3 04-Jan-22 4.6 | This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 In seninf driver, there is a possible information disclosure due to | This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 In seninf driver, there is a possible information disclosure due to hettps://corp. mediatek.com/product-security-bulletin/Janu ary-2022 |

| Weakness | Publish Date | cvss | 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: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | bulletin/Janu ary-2022 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/304 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/305 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection | https://corp. mediatek.com /product- security- | H-MED- MT81- 210122/306 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | bulletin/Janu ary-2022 | |
| | | | CVE ID : CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/307 |
| mt8167s | | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/308 |

| Weakness | Publish Date | cvss | Descriptio | n & CVE ID | P | atch | NCI | IPC ID |
|---|---------------|------|--|--|--|----------------|----------------------|--------|
| | | | ALPS06198513 | 3. | | | | |
| | | | CVE ID : CVE-2 | 2022-20021 | | | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, the possible link did due to bluetooth properly handle attempt from a same BD addressurrently conn. This could lead denial of service with no addition privileges need interaction is nexploitation. Para ALPS06198578 | isconnection th does not e a connection host with the ess as the ected BT host. I to remote the of bluetooth onal execution led. User lot needed for atch ID: B; Issue ID: | https: media /prod securi | ty- in/Janu | H-ME MT81 2101 | |
| | | | CVE ID : CVE-2 | 2022-20022 | | | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not | | media /prod securi bullet ary-20 | ty- in/Janu | H-ME MT81 2101 | |
| mt8168 | | | | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User | | media /prod securi | ty- in/Janu | H-ME MT81 2101 | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 | 4-5 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/312 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/313 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/314 |

0-1

2-3 3-4 4-5 5-6

6-7 7-8

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|--------------|------|---|--|-------------------------------|
| | | | ID: ALPS06198608; Issue ID: ALPS06198608. | | |
| | | | CVE ID : CVE-2022-20023 | | |
| mt8169 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/315 |
| | | | CVE ID : CVE-2022-20012 | | |
| Improper Initialization | 04-Jan-22 | 2.1 | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. CVE ID: CVE-2022-20015 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/316 |
| mt8173 | | | 0VE1D 1 0VE 2022 20013 | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/317 |

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | ALPS05836478; Issue ID: ALPS05836478. | | |
| | | | CVE ID : CVE-2022-20012 | | |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/318 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/319 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/320 |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | ALPS06198513; Issue ID: ALPS06198513. | | |
| | | | CVE ID : CVE-2022-20021 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/321 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/322 |
| mt8175 | | | | | |
| Missing Release of Resource after Effective Lifetime CVSS Scoring Sc. | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/323 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--------------------------------------|--------------|------|--|--|-------------------------------|
| | | | bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | | |
| mt8183 | | | CVE ID: CVE-2022-20023 | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/324 |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/325 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/326 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|--|--|-------------------------------|
| | | | denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/327 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/328 |
| mt8185 | | | | | |
| Concurrent | 04-Jan-22 | 4.4 | In vow driver, there is a | https://corp. | H-MED- |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-1 0 |

| Validation | 4-Jan-22 | | possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 In vow driver, there is a possible memory corruption due to improper input | mediatek.com /product- security- bulletin/Janu ary-2022 | MT81- 210122/329 |
|---|----------|-----|--|--|-------------------------------|
| Input 04 Validation Improper 04 | 4-Jan-22 | | possible memory corruption due to improper input | | |
| 1 1 ()4 | | 4.6 | validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/330 |
| | 4-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/331 |
| Improper Restriction of Operations within the Bounds of a | 4-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with no additional | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/332 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Memory Buffer | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05943906; Issue ID: ALPS05943906. | | |
| | | | CVE ID : CVE-2022-20020 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/333 |
| | | | CVE ID : CVE-2022-20023 | | |
| mt8188 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT81- 210122/334 |
| | | | CVE ID : CVE-2022-20012 | | |
| mt8195 | | | In made duite-on the are to a | https://sees | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with | https://corp. mediatek.com /product- security- bulletin/Janu | H-MED- MT81- 210122/335 |

0-1

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------------|------|--|--|-------------------------------|
| | | | no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | ary-2022 | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patc ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | | H-MED- MT81- 210122/336 |
| mt8321 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/337 |
| Improper Restriction of Operations within the Bounds of a | 04-Jan-22 le 0-1 | 2.1 | In libvcodecdrv, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with no additional 2-3 3-4 4-5 5-6 | bulletin/Janu | H-MED- MT83- 210122/338 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|------------------|--------------|------|--|--|-------------------------------|
| Memory Buffer | | | execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/339 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/340 |
| Missing | 0.4.1 | 0.0 | CVE ID: CVE-2022-20022 In Bluetooth, there is a | https://corp. | H-MED- |
| Release of | 04-Jan-22 | 3.3 | possible application crash | mediatek.com | MT83- |

6-7 7-8

8-9

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|----------------|------|--|--|-------------------------------|
| Resource after Effective Lifetime | | | due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | /product- security- bulletin/Janu ary-2022 | 210122/341 |
| mt8362a | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/342 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, 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 not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/343 |
| Improper | | | In libvcodecdrv, there is a | https://corp. | H-MED- |
| Restriction of | 04-Jan-22 | 2.1 | possible information disclosure due to a missing | mediatek.com /product- | MT83- 210122/344 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| Operations within the Bounds of a Memory Buffer | | | bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | security- bulletin/Janu ary-2022 | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/345 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/346 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | CVE ID : CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/347 |
| mt8362b | | | 0.212.002.002 | | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/348 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/349 |
| CVSS Scoring Sc | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|----------------|------|---|--|-------------------------------|
| | | | with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/350 |
| mt8365 | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/351 |
| Use of Uninitialized Resource | 04-Jan-22 | 2.1 | In seninf driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/352 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Operations within the Bounds of a Memory Buffer Missing Release of Resource after Effective Lifetime O4-Jan-22 O4-Jan-24 O4-Jan-24 O4-Jan-24 O4-Jan-24 O4-Jan-24 O4-Jan-24 O4-Jan- | Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--|--------------|------|---|---|-------------------------------|
| Improper Restriction of Operations within the Bounds of a Memory Buffer Missing Release of Resource after Effective Lifetime O4-Jan-22 O4-Ja | | | | User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. | | |
| Missing Release of Resource after Effective Lifetime O4-Jan-22 GA-Jan-22 In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | Restriction of Operations within the Bounds of a Memory | 04-Jan-22 | 2.1 | possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. | mediatek.com /product- security- bulletin/Janu | H-MED- MT83- 210122/353 |
| mt8385 | Release of Resource after Effective | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | mediatek.com /product- security- bulletin/Janu | H-MED- MT83- 210122/354 |
| | mt8385 | | | | | |
| Overflow or 04-Jan-22 4.6 This could lead to local /product- | Overflow or | 04-Jan-22 | 4.6 | possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution | mediatek.com /product- security- bulletin/Janu | H-MED- MT83- 210122/355 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. | | |
| | | | CVE ID : CVE-2022-20012 | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/356 |
| | | | CVE ID : CVE-2022-20014 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/357 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT83- 210122/358 |

| Weakness | Publish Date | CVSS | | Description | n & CVE | ID | Pa | atch | NCI | IPC ID |
|---|---------------|------|---|--|----------------------------|---------------|--|---------------|----------------------|--------|
| | | | exploi ALPS(ALPS(| ction is r tation. P 0619851 0619851 D : CVE- 2 | atch ID: 3; Issue 3. | ID: | | | | |
| N/A | 04-Jan-22 | 3.3 | In Blu possib due to prope attem same currer This c denial with r privile intera exploi ALPSO | Currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 In Bluetooth, there is a | | | media /prodi securi | ty- n/Janu | H-ME MT83 2101 | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | Dacket. This could lead to | | media /prod securi | ty- n/Janu | H-ME MT83 2101 | | | |
| mt8765 | | | 1 | | | | | | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | possib due to | In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local | | | https://corp. mediatek.com /product- security- | | H-ME MT87 2101 | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | bulletin/Janu ary-2022 | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/362 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/363 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection | https://corp. mediatek.com /product- security- | H-MED- MT87- 210122/364 |

0-1

| Weakness | Publish Date | cvss | Descript | ion & CVE II |) | Pa | itch | NCIII | PC ID |
|---|----------------|------|--|--|---------------|---------------------------|---------------|-------------------------|-------|
| | | | same BD addicurrently con This could leadenial of servith no addit privileges need interaction is exploitation. ALPS061985 | attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 In Bluetooth, there is a | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, possible appl due to blueto device with L packet. This cremote denia bluetooth wit execution pri User interaction pri User interaction and the second of the | media /prodi | ty- n/Janu | H-MEI MT87- 21012 | | | |
| mt8766 | | | | | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. | | | media /prodi securi | ty- n/Janu | H-MEI MT87- 21012 | |
| Missing | 04-Jan-22 | 3.3 | In Bluetooth, | there is a | | https:/ | //corp. | H-MEI |)- |
| CVSS Scoring Sca | nle 0-1 | 1-2 | 2-3 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------|------|---|--|-------------------------------|
| Release of Resource after Effective Lifetime | | | possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | mediatek.com /product- security- bulletin/Janu ary-2022 | MT87- 210122/367 |
| mt8768 | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/368 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/369 |
| Missing Release of | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash | https://corp. mediatek.com | H-MED- MT87- |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 126 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Resource after Effective Lifetime | | | due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | /product- security- bulletin/Janu ary-2022 | 210122/370 |
| mt8786 | | | C. Z.Z. G.Z. ZVZZ MOVMO | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/371 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/372 |
| mt8788 | | | | | |

| Integer | | | In mdp driver, there is a | | |
|---|-----------|-----|---|--|-------------------------------|
| Overflow or Wraparound | 04-Jan-22 | 4.6 | possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. CVE ID: CVE-2022-20012 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/373 |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/374 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdry, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/375 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not | https://corp. mediatek.com /product- | H-MED- MT87- 210122/376 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|--|-------------------------------|
| | | | properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | security- bulletin/Janu ary-2022 | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. CVE ID: CVE-2022-20022 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/377 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/378 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| | | | CVE ID : CVE-2022-20023 | | |
| mt8789 | 1 | | | 1 | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/379 |
| Improper Input Validation | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption 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: ALPS05857308; Issue ID: ALPS05857308. CVE ID: CVE-2022-20014 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/380 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/381 |
| Improper Restriction | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information | https://corp. mediatek.com | H-MED- MT87- |

0-1

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|--|-------------------------------|
| of Operations within the Bounds of a Memory Buffer | | | disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | /product- security- bulletin/Janu ary-2022 | 210122/382 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/383 |
| mt8791 | | | | | |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/384 |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation | https://corp. mediatek.com /product- security- | H-MED- MT87- 210122/385 |

| Weakness | Publish Date | CVSS | Descri | ption & CVE | ID | Pa | tch | NCI | IPC ID |
|---|--------------|------|---|--|--|-------------------|----------------------------------|-----------------------|--------|
| | | | of privilege execution p User intera needed for ID: ALPS05 ALPS05862 CVE ID: CV | orivileges n ction is not exploitatio 862986; Is 2986. | eeded. n. Patch sue ID: | bulleti ary-20 | n/Janu 22 | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcode possible in disclosure bounds che to local info disclosure execution puser interaneeded for ID: ALPS05943 | formation due to a mieck. This continuous ormation with no addition is not exploitation 943906; Is 3906. | ssing uld lead ditional eeded. t n. Patch sue ID: | media /prodi | ty- n/Janu | H-ME MT87 2101 | |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not | | media /prodi | ty- n/Janu | H-ME MT87 2101 | | |
| mt8797 | | | | | | L | | L | |
| Concurrent Execution using Shared Resource with Improper CVSS Scoring Sca | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. 2-3 3-4 4-5 5-6 | | corruption mediatek.com dition. This /product- al escalation security- System bulletin/Janu ges needed. ary-2022 | | tek.com uct- ty- n/Janu | H-ME MT87 21012 | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Synchronizat ion ('Race Condition') | | | User interaction is not needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05837742. CVE ID: CVE-2022-20013 | | |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. CVE ID: CVE-2022-20016 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/389 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/390 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | H-MED- MT87- 210122/391 |

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|--|-------------------------------|
| | | | ALPS06198608. | | |
| | | | CVE ID : CVE-2022-20023 | | |
| Samsung | | | | | |
| exynos | | | | | |
| Improper Handling of Exceptional Conditions | 10-Jan-22 | 4.6 | An improper check or handling of exceptional conditions in NPU driver prior to SMR Jan-2022 Release 1 allows arbitrary memory write and code execution. CVE ID: CVE-2022-22265 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | H-SAM- EXYN- 210122/392 |
| | | | | | |
| aluinaliuuu | | | Operating System | | |
| alpinelinux | | | | | |
| alpine_linux | T | | | | |
| Improper Privilege Management | 06-Jan-22 10 | | The zabbix-agent2 package before 5.4.9-r1 for Alpine Linux sometimes allows privilege escalation to root because the design incorrectly expected that systemd would (in effect) determine part of the configuration. CVE ID: CVE-2022-22704 | https://gitlab .alpinelinux.o rg/alpine/ap orts/- /issues/1336 8 | O-ALP-ALPI- 210122/393 |
| Debian | | | CVE ID . CVE-2022-22704 | | |
| debian_linux | | | | | |
| acbiun_iiiux | | | In lighttpd 1.4.46 through | | |
| Out-of- bounds Write | 06-Jan-22 | 4.3 | 1.4.63, the mod_extforward_Forwarded function of the mod_extforward plugin has a stack-based buffer overflow (4 bytes representing -1), as demonstrated by remote denial of service (daemon crash) in a non-default | https://redmi ne.lighttpd.ne t/issues/313 4 | O-DEB- DEBI- 210122/394 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| | | | configuration. The non-default configuration requires handling of the Forwarded header in a somewhat unusual manner. Also, a 32-bit system is much more likely to be affected than a 64-bit system. CVE ID: CVE-2022-22707 | | |
| Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection') | 06-Jan-22 | 5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain way. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this vulnerability. CVE ID: CVE-2022-21661 | https://githu b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA- 6676-cqfm- gw84, https://word press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, https://githu b.com/Word Press/wordp ress- develop/com mit/17efac8c 8ec64555eff5 cf51a3eff81e 06317214 | O-DEB- DEBI- 210122/395 |
| Improper Neutralizatio n of Input During Web Page Generation ('Cross-site | 06-Jan-22 | 3.5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Lowprivileged authenticated users (like author) in | https://word press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, https://githu | O-DEB- DEBI- 210122/396 |

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|-------------------------------|
| Scripting') | | | WordPress core are able to execute JavaScript/perform stored XSS attack, which can affect high-privileged users. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. CVE ID: CVE-2022-21662 | b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA- 699q-3hj9- 889w | |
| Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection') | 06-Jan-22 | 6.5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. | https://word press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, https://githu b.com/Word Press/wordp ress- develop/secu rity/advisorie s/GHSA- jmmq-m8p8- 332h | O-DEB- DEBI- 210122/397 |
| Improper Neutralizatio n of Special Elements used in an SQL | 06-Jan-22 | 6.5 | WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in | https://word press.org/ne ws/2022/01/ wordpress-5- 8-3-security- release/, | O-DEB- DEBI- 210122/398 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|----------------|------|--|--|-------------------------------|
| Command ('SQL Injection') | | | one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue. CVE ID: CVE-2022-21664 | gw8h-6x86 | |
| Google | | | | | |
| android | | | | | |
| Improper Privilege Management | 10-Jan-22 | 2.1 | Unprotected dynamic receiver in SecSettings prior to SMR Jan-2022 Release 1 allows untrusted applications to launch arbitrary activity. CVE ID: CVE-2022-22263 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/399 |
| Improper Input Validation | 10-Jan-22 | 3.6 | Improper sanitization of incoming intent in Dressroom prior to SMR Jan-2022 Release 1 allows local attackers to read and write arbitrary files without permission. CVE ID: CVE-2022-22264 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/400 |
| Improper Handling of Exceptional Conditions | 10-Jan-22 | 4.6 | An improper check or handling of exceptional conditions in NPU driver prior to SMR Jan-2022 Release 1 allows arbitrary memory write and code execution. CVE ID: CVE-2022-22265 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/401 |
| Improper | 10-Jan-22 | 2.1 | (Applicable to China models | https://secur | 0-G00- |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| Privilege Management | | | only) Unprotected WifiEvaluationService in TencentWifiSecurity application prior to SMR Jan- 2022 Release 1 allows untrusted applications to get WiFi information without proper permission. CVE ID: CVE-2022-22266 | ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | ANDR- 210122/402 |
| Files or Directories Accessible to External Parties | 10-Jan-22 | 2.1 | Implicit Intent hijacking vulnerability in ActivityMetricsLogger prior to SMR Jan-2022 Release 1 allows attackers to get running application information. CVE ID: CVE-2022-22267 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/403 |
| Files or Directories Accessible to External Parties | 10-Jan-22 | 3.6 | Incorrect implementation of Knox Guard prior to SMR Jan-2022 Release 1 allows physically proximate attackers to temporary unlock the Knox Guard via Samsung DeX mode. CVE ID: CVE-2022-22268 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/404 |
| Files or Directories Accessible to External Parties | 10-Jan-22 | 2.1 | Keeping sensitive data in unprotected BluetoothSettingsProvider prior to SMR Jan-2022 Release 1 allows untrusted applications to get a local Bluetooth MAC address. CVE ID: CVE-2022-22269 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/405 |
| Files or Directories Accessible to External Parties | 10-Jan-22 | 4.3 | An implicit Intent hijacking vulnerability in Dialer prior to SMR Jan-2022 Release 1 allows unprivileged applications to access contact | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 | O-GOO- ANDR- 210122/406 |

2-3 3-4 4-5 5-6

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|--|-------------------------------|
| | | | information. | 22&month=1 | |
| | | | CVE ID : CVE-2022-22270 | | |
| Improper Input Validation | 10-Jan-22 | 2.1 | A missing input validation before memory copy in TIMA trustlet prior to SMR Jan-2022 Release 1 allows attackers to copy data from arbitrary memory. CVE ID: CVE-2022-22271 | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/407 |
| Incorrect Authorizatio n | 10-Jan-22 | 2.1 | Improper authorization in TelephonyManager prior to SMR Jan-2022 Release 1 allows attackers to get IMSI without READ_PRIVILEGED_PHONE_S TATE permission | https://secur ity.samsungm obile.com/sec urityUpdate.s msb?year=20 22&month=1 | O-GOO- ANDR- 210122/408 |
| | | | CVE ID : CVE-2022-22272 | | |
| Integer Overflow or Wraparound | 04-Jan-22 | 4.6 | In mdp driver, there is a possible memory corruption 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: ALPS05836478; Issue ID: ALPS05836478. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | 0-G00- ANDR- 210122/409 |
| Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition') | 04-Jan-22 | 4.4 | In vow driver, there is a possible memory corruption 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: ALPS05837742; Issue ID: | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | O-GOO- ANDR- 210122/410 |

2-3 3-4 4-5 5-6

| Weakness | Publish Date | CVSS | | Description | n & CVE | ID | Pa | tch | NCI | IPC ID |
|---------------------------------|----------------|------|--|---|--|----------------------------|----------------------------|------------------------|------------------------|--------|
| | | | ALPS0 | 5837742 | 2. | | | | | |
| | | | CVE II |) : CVE-2 | 022-20 | 0013 | | | | |
| Improper Input Validation | 04-Jan-22 | 4.6 | possib due to validat local e with Sy privile interac exploit ALPSO ALPSO | driver, to | ry correct input so could less of prived ecution led. Use ot need atch ID: 3; Issue 3. | lead to ilege red for ID: | media /produ securit | ty- n/Janu | O-GO ANDF 21012 | |
| Improper Initialization | 04-Jan-22 | 2.1 | there is informuninitial lead to discloss execute User in needed ID: ALM | In kd_camera_hw driver, 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 not needed for exploitation. Patch ID: ALPS05862966. | | | media /produ securit | ty- n/Janu | O-GO(ANDR 21012 | |
| Improper Locking | 04-Jan-22 | 4.6 | In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986. | | | media /produ securit | ty- n/Janu | 0-G00 ANDR 21012 | _ | |
| Use of | 04-Jan-22 | 2.1 | In seninf driver, there is a | | | https://corp. | | 0-G0 | | |
| Uninitialized | , | | | le inform | | | l . | tek.com | ANDR | |
| CVSS Scoring Sca | ile 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|---|--|-------------------------------|
| Resource | | | disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. CVE ID: CVE-2022-20018 | /product- security- bulletin/Janu ary-2022 | 210122/414 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. CVE ID: CVE-2022-20019 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | O-GOO- ANDR- 210122/415 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 04-Jan-22 | 2.1 | In libvcodecdrv, there is a possible information disclosure 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: ALPS05943906; Issue ID: ALPS05943906. CVE ID: CVE-2022-20020 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | O-GOO- ANDR- 210122/416 |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple | https://corp. mediatek.com /product- security- bulletin/Janu | O-GOO- ANDR- 210122/417 |

0-1

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|--|-------------------------------|
| | | | LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513. CVE ID: CVE-2022-20021 | ary-2022 | |
| N/A | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578. | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | O-GOO- ANDR- 210122/418 |
| Missing Release of Resource after Effective Lifetime | 04-Jan-22 | 3.3 | In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608. CVE ID: CVE-2022-20023 | https://corp. mediatek.com /product- security- bulletin/Janu ary-2022 | O-GOO- ANDR- 210122/419 |

6-7 7-8

8-9

CVSS Scoring Scale

| Weakness | Publish Date | cvss | Des | scriptio | n & CVE | ID | Pa | atch | NCI | PC ID |
|--|----------------|------|---|---|---------|-----------------------------|---|--|------------------------|-------|
| Microsoft | | | | | | | | | | |
| windows_10 | | | | | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Elevation Vulnerab | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | | | | //porta .micros m/en- curity- nce/adv CVE- 21833 | O-MI(WINE 21012 | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | | | | l.msrc oft.cor US/se | curity- nce/adv CVE- | O-MI(WIND 21012 | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | | | l.msrc. oft.cor US/se | curity- nce/adv CVE- | 0-MI(WINE 21012 | | |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | | | l.msrc. oft.cor US/se | curity- nce/adv CVE- | O-MI(WINE 21012 | | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | | | | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | | O-MIC WIND 21012 | |
| Uncontrolled Resource | 11-Jan-22 | 2.1 | Window: Discretion | | | | | //porta micros | O-MIC WIND | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---------------------|------|--|---|-------------------------------|
| Consumption | | | List Denial of Service Vulnerability. CVE ID: CVE-2022-21839 | oft.com/en- US/security- guidance/adv isory/CVE- 2022-21839 | 210122/425 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/426 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.9 | Windows Hyper-V Denial of Service Vulnerability. CVE ID: CVE-2022-21847 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21847 | O-MIC- WIND- 210122/427 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/428 |
| N/A | 11-Jan-22 | 9.3 | Windows IKE Extension Remote Code Execution Vulnerability. CVE ID: CVE-2022-21849 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21849 | O-MIC- WIND- 210122/429 |
| N/A CVSS Scoring Sca | 11-Jan-22 le 0-1 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- | https://porta l.msrc.micros oft.com/en- US/security- | O-MIC- WIND- 210122/430 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|--|---|-------------------------------|
| | | | 21851. CVE ID : CVE-2022-21850 | guidance/adv isory/CVE- 2022-21850 | |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | O-MIC- WIND- 210122/431 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022- 21896, CVE-2022-21902. CVE ID: CVE-2022-21852 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21852 | O-MIC- WIND- 210122/432 |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21857 | O-MIC- WIND- 210122/433 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows Bind Filter Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21858 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21858 | O-MIC- WIND- 210122/434 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Accounts Control Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21859 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | O-MIC- WIND- 210122/435 |
| Improper | 11-Jan-22 | 7.2 | Task Flow Data Engine | https://porta | O-MIC- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|---------------|------|--|---|-------------------------------|
| Privilege Management | | | Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21861 | l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21861 | WIND- 210122/436 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/437 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows StateRepository API Server file Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21863 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21863 | O-MIC- WIND- 210122/438 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Push Notifications Apps Elevation Of Privilege Vulnerability. CVE ID: CVE-2022-21867 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21867 | O-MIC- WIND- 210122/439 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Devices Human Interface Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21868 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21868 | O-MIC- WIND- 210122/440 |
| windows_11 | | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. | https://porta l.msrc.micros oft.com/en- US/security- | O-MIC- WIND- 210122/441 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 1/16 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|---------------|------|--|---|-------------------------------|
| | | | CVE ID : CVE-2022-21833 | guidance/adv isory/CVE- 2022-21833 | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21834 | O-MIC- WIND- 210122/442 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21835 | O-MIC- WIND- 210122/443 |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21836 | O-MIC- WIND- 210122/444 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/445 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/446 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|-------------------------------|
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.9 | Windows Hyper-V Denial of Service Vulnerability. CVE ID: CVE-2022-21847 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21847 | O-MIC- WIND- 210122/447 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/448 |
| N/A | 11-Jan-22 | 9.3 | Windows IKE Extension Remote Code Execution Vulnerability. CVE ID: CVE-2022-21849 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21849 | O-MIC- WIND- 210122/449 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. CVE ID: CVE-2022-21850 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21850 | O-MIC- WIND- 210122/450 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | O-MIC- WIND- 210122/451 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is | https://porta l.msrc.micros oft.com/en- | O-MIC- WIND- 210122/452 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|---------------|------|--|---|-------------------------------|
| | | | unique from CVE-2022- 21896, CVE-2022-21902. CVE ID : CVE-2022-21852 | US/security- guidance/adv isory/CVE- 2022-21852 | |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21857 | O-MIC- WIND- 210122/453 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows Bind Filter Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21858 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21858 | O-MIC- WIND- 210122/454 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Task Flow Data Engine Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21861 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21861 | O-MIC- WIND- 210122/455 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/456 |
| windows_7 | | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- | O-MIC- WIND- 210122/457 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 149 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | | |
|--|----------------|------|--|---|-------------------------------|--|--|
| | | | | 2022-21833 | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21834 | O-MIC- WIND- 210122/458 | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | rices Elevation of ilege Vulnerability. oft.com/en- US/security- guidance/adv | | | |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21836 | O-MIC- WIND- 210122/460 | | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/461 | | |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/462 | | |
| Uncontrolled Resource | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service | https://porta l.msrc.micros | O-MIC- WIND- | | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|---|---|-------------------------------|
| Consumption | | | Vulnerability. This CVE ID is unique from CVE-2022-21843, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890. CVE ID: CVE-2022-21848 | oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | 210122/463 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. CVE ID: CVE-2022-21850 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21850 | O-MIC- WIND- 210122/464 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | O-MIC- WIND- 210122/465 |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21857 | O-MIC- WIND- 210122/466 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Accounts Control Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21859 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | O-MIC- WIND- 210122/467 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv | O-MIC- WIND- 210122/468 |

0-1

6-7 7-8

8-9

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|---|-------------------------------|
| | | | | isory/CVE- 2022-21862 | |
| windows_8.1 | | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21833 | O-MIC- WIND- 210122/469 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21834 | O-MIC- WIND- 210122/470 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21835 | O-MIC- WIND- 210122/471 |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21836 | O-MIC- WIND- 210122/472 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/473 |

| Weakness | Publish Date | CVSS | Description | n & CVE ID | | Pa | itch | NCII | PC ID |
|---|----------------|------|--|--|------------------------------|------------------------------|----------------------------|------------------------|-------|
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE E Denial of Service Vulnerability. To unique from CV 21848, CVE-20 CVE-2022-2188 21890. CVE ID: CVE-2 | ce 'his CVE II /E-2022- 22-21883 89, CVE-20 | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MI(WIND 21012 | | |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE E Denial of Service Vulnerability. To unique from CV 21843, CVE-20 CVE-2022-2188 21890. CVE ID: CVE-2 | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIC WIND 21012 | | | |
| N/A | 11-Jan-22 | 9.3 | Remote Code E Vulnerability. T unique from CV 21851. | ote Desktop Client Ote Code Execution Oterability. This CVE ID is OTERE OF THE ID IS OTER | | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIC WIND 21012 | |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIO WIND 21012 | | |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | | | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIC WIND 21012 | |
| Improper Privilege | 11-Jan-22 | 6.9 | Windows Accor Elevation of Pri | | rol | | //porta micros | O-MIC WIND | |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|---------------|------|--|---|-------------------------------|
| Management | | | Vulnerability. CVE ID: CVE-2022-21859 | oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | 210122/479 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/480 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Push Notifications Apps Elevation Of Privilege Vulnerability. CVE ID: CVE-2022-21867 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21867 | O-MIC- WIND- 210122/481 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Devices Human Interface Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21868 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21868 | O-MIC- WIND- 210122/482 |
| windows_serv | ver | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21833 | O-MIC- WIND- 210122/483 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv | O-MIC- WIND- 210122/484 |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 154 of 169 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|---|-------------------------------|
| | | | CVE ID : CVE-2022-21834 | isory/CVE- 2022-21834 | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21835 | O-MIC- WIND- 210122/485 |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21836 | O-MIC- WIND- 210122/486 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/487 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/488 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.9 | Windows Hyper-V Denial of Service Vulnerability. CVE ID: CVE-2022-21847 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21847 | O-MIC- WIND- 210122/489 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|-------------------------------|
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/490 |
| N/A | 11-Jan-22 | 9.3 | Windows IKE Extension Remote Code Execution Vulnerability. CVE ID: CVE-2022-21849 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21849 | O-MIC- WIND- 210122/491 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. CVE ID: CVE-2022-21850 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21850 | O-MIC- WIND- 210122/492 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | O-MIC- WIND- 210122/493 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022- 21896, CVE-2022-21902. CVE ID: CVE-2022-21852 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21852 | O-MIC- WIND- 210122/494 |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. | https://porta l.msrc.micros oft.com/en- | O-MIC- WIND- 210122/495 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|--|---|-------------------------------|
| | | | CVE ID : CVE-2022-21857 | US/security- guidance/adv isory/CVE- 2022-21857 | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows Bind Filter Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21858 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21858 | O-MIC- WIND- 210122/496 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Accounts Control Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21859 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | O-MIC- WIND- 210122/497 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Task Flow Data Engine Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21861 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21861 | O-MIC- WIND- 210122/498 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/499 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows StateRepository API Server file Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21863 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21863 | O-MIC- WIND- 210122/500 |

6-7 7-8

8-9

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|---------------------------------------|----------------|------|---|---|-------------------------------|
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Push Notifications Apps Elevation Of Privilege Vulnerability. CVE ID: CVE-2022-21867 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21867 | O-MIC- WIND- 210122/501 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Devices Human Interface Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21868 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21868 | O-MIC- WIND- 210122/502 |
| windows_serv | ver_2008 | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21833 | O-MIC- WIND- 210122/503 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21834 | O-MIC- WIND- 210122/504 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21835 | O-MIC- WIND- 210122/505 |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. | https://porta l.msrc.micros oft.com/en- | O-MIC- WIND- 210122/506 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|---------------------|------|--|---|-------------------------------|
| | | | CVE ID : CVE-2022-21836 | US/security- guidance/adv isory/CVE- 2022-21836 | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/507 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/508 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/509 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. CVE ID: CVE-2022-21850 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21850 | O-MIC- WIND- 210122/510 |
| N/A CVSS Scoring Sca | 11-Jan-22 le 0-1 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv | O-MIC- WIND- 210122/511 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|---|---|-------------------------------|
| | | | 21850. CVE ID : CVE-2022-21851 | isory/CVE- 2022-21851 | |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21857 | O-MIC- WIND- 210122/512 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/513 |
| windows_serv | ver_2012 | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21833 | O-MIC- WIND- 210122/514 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21834 | O-MIC- WIND- 210122/515 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21835 | O-MIC- WIND- 210122/516 |

0-1

6-7 7-8 8-9

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|--|---|-------------------------------|
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21836 | O-MIC- WIND- 210122/517 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID : CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/518 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/519 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/520 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. CVE ID: CVE-2022-21850 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21850 | O-MIC- WIND- 210122/521 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution | https://porta l.msrc.micros | O-MIC- WIND- |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|--|---|-------------------------------|
| | | | Vulnerability. This CVE ID is unique from CVE-2022-21850. CVE ID: CVE-2022-21851 | oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | 210122/522 |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21857 | O-MIC- WIND- 210122/523 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Accounts Control Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21859 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | O-MIC- WIND- 210122/524 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/525 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Push Notifications Apps Elevation Of Privilege Vulnerability. CVE ID: CVE-2022-21867 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21867 | O-MIC- WIND- 210122/526 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Devices Human Interface Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21868 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- | O-MIC- WIND- 210122/527 |

0-1

6-7 7-8 8-9

| Weakness | Publish Date | CVSS | Description | & CVE ID | Pa | tch | NCII | PC ID | | |
|--|---------------------|------|---|-----------------------|------------------------------|----------------------------|------------------------|-------|--|--|
| | | | | | 2022-2 | 21868 | | | | |
| windows_serv | windows_server_2016 | | | | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine Elevation of Priv Vulnerability. | ilege | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIO WIND 21012 | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-m Framework Reflection of Priv Vulnerability. CVE ID: CVE-20 | ector Driver ilege | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIO WIND 21012 | | | |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Crypto Services Elevatio Privilege Vulnera CVE ID: CVE-20 | on of ability. | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MI(WIND 21012 | | | |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certific Vulnerability. CVE ID : CVE-20 | . 0 | l.msrc. oft.con US/sec | curity- ice/adv CVE- | O-MIC WIND 21012 | | | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Vulnerability. CVE ID: CVE-2022-21838 US/security- guidance/adv isory/CVE- 2022-21838 | | O-MIC WIND 21012 | | | | | |
| Uncontrolled Resource | 11-Jan-22 | 4.3 | Windows IKE Ex Denial of Service | | | //porta micros | O-MIO WIND | | | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 | 4-5 5-6 | 6-7 | 7-8 | 8-9 | 9-10 | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|-------------------------------|
| Consumption | | | Vulnerability. This CVE ID is unique from CVE-2022-21848, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890. CVE ID: CVE-2022-21843 | oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | 210122/533 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/534 |
| N/A | 11-Jan-22 | 9.3 | Windows IKE Extension Remote Code Execution Vulnerability. CVE ID: CVE-2022-21849 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21849 | O-MIC- WIND- 210122/535 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. CVE ID: CVE-2022-21850 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21850 | O-MIC- WIND- 210122/536 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | O-MIC- WIND- 210122/537 |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. | https://porta l.msrc.micros oft.com/en- US/security- | O-MIC- WIND- 210122/538 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID | | | | | | |
|-------------------------------------|---------------|------|--|---|-------------------------------|--|--|--|--|--|--|
| | | | CVE ID : CVE-2022-21857 | guidance/adv isory/CVE- 2022-21857 | | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Accounts Control Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21859 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | O-MIC- WIND- 210122/539 | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/540 | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows StateRepository API Server file Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21863 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21863 | O-MIC- WIND- 210122/541 | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Push Notifications Apps Elevation Of Privilege Vulnerability. CVE ID: CVE-2022-21867 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21867 | O-MIC- WIND- 210122/542 | | | | | | |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Devices Human Interface Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21868 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21868 | O-MIC- WIND- 210122/543 | | | | | | |
| windows_serv | ver_2019 | | | | | | | | | | |
| CVSS Scoring Sca | le 0-1 | 1-2 | 2-3 3-4 4-5 5-6 Page 165 of 169 | 6-7 7-8 | CVSS Scoring Scale | | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|--|--------------|------|---|---|-------------------------------|
| Improper Privilege Management | 11-Jan-22 | 7.2 | Virtual Machine IDE Drive Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21833 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21833 | O-MIC- WIND- 210122/544 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21834 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21834 | O-MIC- WIND- 210122/545 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Microsoft Cryptographic Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21835 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21835 | O-MIC- WIND- 210122/546 |
| Improper Certificate Validation | 11-Jan-22 | 7.2 | Windows Certificate Spoofing Vulnerability. CVE ID: CVE-2022-21836 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21836 | O-MIC- WIND- 210122/547 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Jan-22 | 7.2 | Windows Cleanup Manager Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21838 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21838 | O-MIC- WIND- 210122/548 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 2.1 | Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability. | https://porta l.msrc.micros oft.com/en- US/security- | O-MIC- WIND- 210122/549 |

2-3 3-4 4-5 5-6

6-7 7-8 8-9

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|--------------|------|--|---|-------------------------------|
| | | | CVE ID : CVE-2022-21839 | guidance/adv isory/CVE- 2022-21839 | |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.3 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21848, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21843 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21843 | O-MIC- WIND- 210122/550 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 4.9 | Windows Hyper-V Denial of Service Vulnerability. CVE ID: CVE-2022-21847 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21847 | O-MIC- WIND- 210122/551 |
| Uncontrolled Resource Consumption | 11-Jan-22 | 7.1 | Windows IKE Extension Denial of Service Vulnerability. This CVE ID is unique from CVE-2022- 21843, CVE-2022-21883, CVE-2022-21889, CVE-2022- 21890. CVE ID: CVE-2022-21848 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21848 | O-MIC- WIND- 210122/552 |
| N/A | 11-Jan-22 | 9.3 | Windows IKE Extension Remote Code Execution Vulnerability. CVE ID: CVE-2022-21849 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21849 | O-MIC- WIND- 210122/553 |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21851. | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- | O-MIC- WIND- 210122/554 |

| Weakness | Publish Date | cvss | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|----------------|------|--|---|-------------------------------|
| | | | CVE ID : CVE-2022-21850 | 2022-21850 | |
| N/A | 11-Jan-22 | 9.3 | Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022- 21850. CVE ID: CVE-2022-21851 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21851 | O-MIC- WIND- 210122/555 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows DWM Core Library Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022- 21896, CVE-2022-21902. CVE ID: CVE-2022-21852 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21852 | O-MIC- WIND- 210122/556 |
| Improper Privilege Management | 11-Jan-22 | 9 | Active Directory Domain Services Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21857 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21857 | O-MIC- WIND- 210122/557 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Windows Bind Filter Driver Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21858 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21858 | O-MIC- WIND- 210122/558 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Accounts Control Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21859 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21859 | O-MIC- WIND- 210122/559 |
| Improper Privilege Management | 11-Jan-22 | 7.2 | Task Flow Data Engine Elevation of Privilege Vulnerability. | https://porta l.msrc.micros oft.com/en- | O-MIC- WIND- 210122/560 |
| CVSS Scoring Sca | ale 0-1 | 1-2 | 2-3 3-4 4-5 5-6 | 6-7 7-8 | 8-9 9-10 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|-------------------------------------|--------------|------|---|---|-------------------------------|
| | | | CVE ID : CVE-2022-21861 | US/security- guidance/adv isory/CVE- 2022-21861 | |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Application Model Core API Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21862 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21862 | O-MIC- WIND- 210122/561 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows StateRepository API Server file Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21863 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21863 | O-MIC- WIND- 210122/562 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Push Notifications Apps Elevation Of Privilege Vulnerability. CVE ID: CVE-2022-21867 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21867 | O-MIC- WIND- 210122/563 |
| Improper Privilege Management | 11-Jan-22 | 6.9 | Windows Devices Human Interface Elevation of Privilege Vulnerability. CVE ID: CVE-2022-21868 | https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2022-21868 | O-MIC- WIND- 210122/564 |