Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Cisco					
unified_contact_center_express					
Incorrect Resource Transfer Between Spheres	14-Jan-22	8.5	A vulnerability in the web-based 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/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmp-priv-esc-JzhTFLm4	A-CIS-UNIF-210122/1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20658		
unified_contact_center_management_portal					
Incorrect Resource Transfer Between Spheres	14-Jan-22	8.5	A vulnerability in the web-based 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-sa-ccmp-priv-esc-JzhTFLm4	A-CIS-UNIF-210122/2
Codeigniter					
codeigniter					
Deserialization of	04-Jan-22	7.5	CodeIgniter is an open source PHP full-stack web	https://github.com/codeig	A-COD-CODE-

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 auto-loadable 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()`. **CVE ID : CVE-2022-21647**	niter4/CodeIgniter4/commit/ce95ed5765256e2f09f3513e7d42790e0d6948f5, https://github.com/codeigniter4/CodeIgniter4/security/advisories/GHSA-w6jr-wj64-mc9x	210122/3
convos					
convos					
Improper Neutralization 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://github.com/convos-chat/convos/security/advisories/GHSA-xmpj-xwm3-vww7, https://github.com/convos-chat/convos/commit/86b2193de375005ba71d9dd53843562c6ac1847c, https://www.	A-CON-CONV-210122/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				huntr.dev/bounties/4532a0ac-4e7c-4fcf-9fe3-630e132325c0/	
Improper Neutralization 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**	https://github.com/convos-chat/convos/security/advisories/GHSA-mm2v-4v7g-m695, https://github.com/convos-chat/convos/commit/5c0a1ec9a2c147bc3b63fd5a48da5f32e18fe5df, https://www.huntr.dev/bounties/ae424798-de01-4972-b73b-2db674f82368/	A-CON-CONV-210122/5
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			still have access to the application even after the password was changed. **CVE ID : CVE-2022-22113**		
daybyday_crm					
Missing Authorization	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 appointments of all users in the system including administrators. However, this type of user is not authorized to view the calendar at all. **CVE ID : CVE-2022-22107**	https://github.com/Bottelet/DaybydayCRM/commit/a0392f4a4a14e1e3fedaf6817aefce69b6bd661b	A-DAY-DAYB-210122/7
Missing Authorization	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://github.com/Bottelet/DaybydayCRM/commit/fe842ea5ede237443f1f45a99aeb839133115d8b	A-DAY-DAYB-210122/8
Improper Neutralization 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://github.com/Bottelet/DaybydayCRM/commit/002dc75f400cf307bd00b71a5a93f1e26e52cee2	A-DAY-DAYB-210122/9

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 Requirements	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. **CVE ID : CVE-2022-22110**	https://github.com/Bottelet/DaybydayCRM/commit/a0392f4a4a14e1e3fedaf6817aefce69b6bd661b	A-DAY-DAYB-210122/10
Missing Authorization	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://github.com/Bottelet/DaybydayCRM/commit/fe842ea5ede237443f1f45a99aeb839133115d8b	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://github.com/digitalbazaar/forge/commit/db8016c805371e	A-DIG-FORG-210122/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				72b06d8e2edfe0ace0df934a5e, https://huntr.dev/bounties/41852c50-3c6d-4703-8c55-4db27164a4ae	
discourse					
discourse					
Exposure of Sensitive Information to an Unauthorized 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://github.com/discourse/discourse/commit/702685b6a06ae45a544fc702027f1e4573d94aaa, https://github.com/discourse/discourse/security/advisories/GHSA-mx3h-vc7w-r9c6	A-DIS-DISC-210122/13
Dolibarr					
dolibarr					
Improper Neutralization 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 Neutralization 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 Neutralization 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://github.com/chocobozzz/peertube/commit/7b54a81cccf6b4c12269e9d6897d608b1a99537a, https://huntr.dev/bounties/77ec5308-5561-4664-af21-d780df2d1e4b	A-FRA-PEER-210122/17

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-9d68107fc0b4, https://github.com/chocobozzz/peertube/commit/795212f7acc690c88c86d0fab8772f6564d59cb8	A-FRA-PEER-210122/18
hoppscotch					
hoppscotch					
Exposure of Sensitive Information to an Unauthorized 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-cae7332a68ee, https://github.com/hoppscotch/hoppscotch/commit/86ef1a4e143ea5bb0c7b309574127cc39d4faa74	A-HOP-HOPP-210122/19
ivanti					
workspace_control					
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://forums.ivanti.com/s/article/A-locally-authenticated	A-IVA-WORK-210122/20

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?language=en_US	
libexpat_project					
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://github.com/libexpat/libexpat/pull/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://github.com/libexpat/libexpat/pull/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

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://redmine.lighttpd.net/issues/3134	A-LIG-LIGH-210122/27
livehelperchat					
live_helper_chat					
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-a31b55090736, https://github.com/livehelperchat/livehelperchat/commit/fbed8728be59040a7218610e72f6	A-LIV-LIVE-210122/28

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21840	A-MIC-EXCE-210122/30
exchange_server					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-	A-MIC-OFFI-210122/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')				guidance/advisory/CVE-2022-21840	
N/A	11-Jan-22	9.3	Microsoft Excel Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21841**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21840	A-MIC-OFFI-210122/35
office_web_apps					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21840	A-MIC-OFFI-210122/36
sharepoint_enterprise_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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-	A-MIC-SHAR-210122/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')				guidance/advisory/CVE-2022-21842	
sharepoint_foundation					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21837	A-MIC-SHAR-210122/39
sharepoint_server					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21842	A-MIC-WORD-210122/42
mruby					
mruby					
Heap-based Buffer	02-Jan-22	7.5	mruby is vulnerable to Heap-	https://huntr.dev/bounties	A-MRU-MRUB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			based Buffer Overflow **CVE ID : CVE-2022-0080**	/59a70392-4864-4ce3-8e35-6ac2111d1e2e, https://github.com/mruby/mruby/commit/28ccc664e5dcd3f9d55173e9afde77c4705a9ab6	210122/43
nette					
latte					
Improper Neutralization 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://github.com/nette/latte/commit/9e1b4f7d70f7a9c3fa6753ffa7d7e450a3d4abb0, https://github.com/nette/latte/security/advisories/GHSA-36m2-8rhx-f36j	A-NET-LATT-210122/44
phoronix-media					
phoronix_test_suite					
Improper Neutralization 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-b5d8-7646c9a7ebbd,	A-PHO-PHOR-210122/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				https://github.com/phoronix-test-suite/phoronix-test-suite/commit/56fd0a3b69fb33c1c90a6017ed735889aaa59486	
rangerstudio					
directus					
Improper Neutralization 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://github.com/directus/directus/commit/ec86d5412d45136915d9b622b4a890dd26932b10	A-RAN-DIRE-210122/46
Improper Neutralization 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://github.com/directus/directus/commit/ec86d5412d45136915d9b622b4a890dd26932b10	A-RAN-DIRE-210122/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shopware					
shopware					
URL Redirection to Untrusted Site ('Open Redirect')	05-Jan-22	5.8	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**	https://github.com/shopware/shopware/commit/a90046c765c57a46c4399dce17bd174253c32886, https://github.com/shopware/shopware/security/advisories/GHSA-c53v-qmrx-93hg, https://docs.shopware.com/en/shopware-5-en/securityupdates/security-update-01-2022	A-SHO-SHOP-210122/48
Insufficient Session Expiration	05-Jan-22	5.5	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 upon a password change, all	https://docs.shopware.com/en/shopware-5-en/securityupdates/security-update-01-2022, https://github.com/shopware/shopware/security/advisories/GHSA-p523-jrph-qjc6,	A-SHO-SHOP-210122/49

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://github.com/shopware/shopware/commit/47ebd126a94f4b019b6fde64c0df3d18d74ef7d0	
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-a567c10828ee, https://github.com/star7th/showdoc/commit/e43df0a190f68aefa272507d3bd54475f566c1db	A-SHO-SHOW-210122/50
sismics					
teedy					
Improper Neutralization 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://github.com/sismics/docs/commit/4951229576d6892dc58ab8c572e73639ca82d80c	A-SIS-TEED-210122/51

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 Neutralization 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://github.com/sismics/docs/commit/4951229576d6892dc58ab8c572e73639ca82d80c	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-d11f762d15e7,	A-SNI-SNIP-210122/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://github.com/snipe/snipe-it/commit/cf14a0222c67472086cd08b2155f045edaf75f2e	
soketi_project					
soketi					
Improper Handling of Exceptional Conditions	10-Jan-22	5	soketi is an open-source 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://github.com/soketi/soketi/security/advisories/GHSA-86ch-6w7v-v6xf, https://github.com/soketi/soketi/commit/4b12efef9c31117c36a0a0f1c3aa32114e86364b	A-SOK-SOKE-210122/54
transloadit					
uppy					
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://github.com/transloadit/uppy/commit/fc137e30a2a3102eb191141f280d5de20dacdf8f,	A-TRA-UPPY-210122/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://huntr.dev/bounties/c1c03ef6-3f18-4976-a9ad-08c251279122	
typelevel					
jawn					
Inadequate Encryption Strength	05-Jan-22	5	Jawn is an open source JSON parser. Extenders of the `org.typelevel.jawn.SimpleFacade` and `org.typelevel.jawn.MutableFacade` 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. **CVE ID : CVE-2022-21653**	https://github.com/typelevel/jawn/pull/390, https://github.com/typelevel/jawn/security/advisories/GHSA-vc89-hccf-rq55	A-TYP-JAWN-210122/56
usoc_project					
usoc					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	04-Jan-22	7.5	USOC is an open source CMS 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	https://github.com/Aaron-Junker/USOC/commit/21e8bfd7a9ab0b7f9344a7a3a7c32a7cdd5a0b69,	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://github.com/Aaron-Junker/USOC/security/advisories/GHSA-fjp4-phjh-jgmc	
Improper Neutralization 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://github.com/Aaron-Junker/USOC/security/advisories/GHSA-89jg-6fr3-9q4h, https://github.com/Aaron-Junker/USOC/commit/06217c66c8f9b114726b21633eabcd88ac9034aa	A-USO-USOC-210122/58
VIM					
vim					
Out-of-bounds Read	06-Jan-22	6.8	vim is vulnerable to Out-of-bounds Read **CVE ID : CVE-2022-0128**	https://github.com/vim/vim/commit/d3a117814d6acbf0dca3eff1a7626843b9b3734a, https://huntr.dev/bounties/63f51299-008a-4112-b85b-1e904aadd4ba	A-VIM-VIM-210122/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Jan-22	4.3	vim is vulnerable to Use After Free **CVE ID : CVE-2022-0156**	https://github.com/vim/vim/commit/9f1a39a5d1cd7989ada2d1cb32f97d84360e050f, https://huntr.dev/bounties/47dded34-3767-4725-8c7c-9dcb68c70b36	A-VIM-VIM-210122/60
Heap-based Buffer Overflow	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-ba9cdbf6738b, https://github.com/vim/vim/commit/5f25c3855071bd7e26255c68bf458b1b5cf92f39	A-VIM-VIM-210122/61
Wordpress					
wordpress					
Improper Neutralization 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	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84, https://word	A-WOR-WORD-210122/62

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/news/2022/01/wordpress-5-8-3-security-release/, https://github.com/WordPress/wordpress-develop/commit/17efac8c8ec64555eff5cf51a3eff81e06317214	
Improper Neutralization 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. **CVE ID : CVE-2022-21662**	https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/, https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w	A-WOR-WORD-210122/63
Improper Neutralization 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://wordpress.org/news/2022/01/wordpress-5-8-3-security-	A-WOR-WORD-210122/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			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**	release/, https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-332h	
Improper Neutralization of Special Elements used in an SQL Command ('SQL 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. 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**	https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/, https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-6x86	A-WOR-WORD-210122/65
Hardware					
mediatek					
awus036nh					
N/A	04-Jan-22	3.3	In Bluetooth, there is a possible application crash	https://corp.mediatek.com	H-MED-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/January-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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT65-210122/68
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
			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/January-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/January-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/January-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					
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/January-2022	H-MED-MT65-210122/72
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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT66-210122/74

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/January-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/January-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

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/January-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/January-2022	H-MED-MT67-210122/78
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/January-2022	H-MED-MT67-210122/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20023		
mt6737					
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/January-2022	H-MED-MT67-210122/80
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/January-2022	H-MED-MT67-210122/81
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/January-2022	H-MED-MT67-210122/82

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/January-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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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/January-2022	H-MED-MT67-210122/88

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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/89
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/January-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/January-2022	H-MED-MT67-210122/91

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/January-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/January-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

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/January-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/January-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

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/January-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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT67-210122/102

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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/103
mt6755					
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/January-2022	H-MED-MT67-210122/104
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/January-2022	H-MED-MT67-210122/105

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/January-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/January-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/January-2022	H-MED-MT67-210122/108

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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/109
mt6757					
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/January-2022	H-MED-MT67-210122/110
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/January-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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/112
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/January-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/January-2022	H-MED-MT67-210122/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/115
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/January-2022	H-MED-MT67-210122/116
mt6757c					
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	https://corp.mediatek.com/product-security-bulletin/Janu	H-MED-MT67-210122/117

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/January-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/January-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/January-2022	H-MED-MT67-210122/120

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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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-

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/January-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/January-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/January-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

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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT67-210122/128

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/January-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/January-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/January-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-

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/January-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/January-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/January-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. **CVE ID : CVE-2022-20019**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/135
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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT67-210122/137

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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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/January-2022	H-MED-MT67-210122/140

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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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/January-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/January-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

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: ALPS05863018; Issue ID: ALPS05863018. **CVE ID : CVE-2022-20018**	security-bulletin/January-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/January-2022	H-MED-MT67-210122/148
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/January-2022	H-MED-MT67-210122/149
N/A	04-Jan-22	3.3	In Bluetooth, there is a possible link disconnection due to bluetooth does not	https://corp.mediatek.com/product-	H-MED-MT67-210122/150

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. **CVE ID : CVE-2022-20022**	security-bulletin/January-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/January-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/January-2022	H-MED-MT67-210122/152

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/January-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/January-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/January-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

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/January-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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT67-210122/158
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-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. **CVE ID : CVE-2022-20018**	bulletin/January-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/January-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/January-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/January-2022	H-MED-MT67-210122/162

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**		
mt6769					
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/January-2022	H-MED-MT67-210122/163
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/January-2022	H-MED-MT67-210122/164
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	https://corp.mediatek.com/product-security-bulletin/January-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/January-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/January-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/January-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/January-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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT67-210122/171

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/January-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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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/January-2022	H-MED-MT67-210122/177

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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/178
mt6781					
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT67-210122/179
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/January-2022	H-MED-MT67-210122/180

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/January-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/January-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/January-2022	H-MED-MT67-210122/183
Improper Restriction of	04-Jan-22	2.1	In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT67-210122/184

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/January-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/January-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/January-2022	H-MED-MT67-210122/186
Concurrent Execution using Shared Resource with	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	https://corp.mediatek.com/product-security-bulletin/Janu	H-MED-MT67-210122/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05837742. **CVE ID : CVE-2022-20013**	ary-2022	
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/January-2022	H-MED-MT67-210122/188
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/January-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/January-2022	H-MED-MT67-210122/190

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/January-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/January-2022	H-MED-MT67-210122/192
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/January-2022	H-MED-MT67-210122/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/194
mt6795					
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/January-2022	H-MED-MT67-210122/195
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. **CVE ID : CVE-2022-20019**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT67-210122/196

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/January-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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT68-210122/198
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/199
Improper	04-Jan-22	4.6	In vow driver, there is a	https://corp.	H-MED-

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/January-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/January-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**	https://corp.mediatek.com/product-security-bulletin/January-2022	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

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/January-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/January-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/January-2022	H-MED-MT68-210122/206

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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT68-210122/207
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/208
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:	https://corp.mediatek.com/product-security-bulletin/January-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. **CVE ID : CVE-2022-20015**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT68-210122/210
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/January-2022	H-MED-MT68-210122/211
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/January-2022	H-MED-MT68-210122/212
Improper Restriction	04-Jan-22	2.1	In libMtkOmxGsmDec, there is a possible information	https://corp.mediatek.com	H-MED-MT68-

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/January-2022	210122/213
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/January-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/January-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

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. **CVE ID : CVE-2022-20012**	security-bulletin/January-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	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/January-2022	H-MED-MT68-210122/218
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/January-2022	H-MED-MT68-210122/219

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**		
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/January-2022	H-MED-MT68-210122/220
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/January-2022	H-MED-MT68-210122/221
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/January-2022	H-MED-MT68-210122/222

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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT68-210122/223
mt6873					
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/January-2022	H-MED-MT68-210122/224
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/225

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/January-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/January-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**	https://corp.mediatek.com/product-security-bulletin/January-2022	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

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/January-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/January-2022	H-MED-MT68-210122/230
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/January-2022	H-MED-MT68-210122/231
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/January-2022	H-MED-MT68-210122/232

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**		
mt6875					
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/January-2022	H-MED-MT68-210122/233
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/January-2022	H-MED-MT68-210122/234
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	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT68-210122/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. **CVE ID : CVE-2022-20019**		
mt6877					
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/January-2022	H-MED-MT68-210122/236
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/237
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/January-2022	H-MED-MT68-210122/238

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/January-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/January-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/January-2022	H-MED-MT68-210122/241
Improper Restriction of	04-Jan-22	2.1	In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT68-210122/242

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/January-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/January-2022	H-MED-MT68-210122/243
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/January-2022	H-MED-MT68-210122/244
mt6883					
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	https://corp.mediatek.com/product-security-	H-MED-MT68-210122/245

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/January-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/246
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/January-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/January-2022	H-MED-MT68-210122/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966. **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/January-2022	H-MED-MT68-210122/249
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/January-2022	H-MED-MT68-210122/250
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/January-2022	H-MED-MT68-210122/251

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/January-2022	H-MED-MT68-210122/252
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-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/January-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

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; Issue ID: ALPS05862966. **CVE ID : CVE-2022-20015**	security-bulletin/January-2022	
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/January-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/January-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/January-2022	H-MED-MT68-210122/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620. **CVE ID : CVE-2022-20019**		
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/January-2022	H-MED-MT68-210122/259
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/January-2022	H-MED-MT68-210122/260
mt6889					
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/January-2022	H-MED-MT68-210122/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478. **CVE ID : CVE-2022-20012**		
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/262
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/January-2022	H-MED-MT68-210122/263
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/January-2022	H-MED-MT68-210122/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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/January-2022	H-MED-MT68-210122/265
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/January-2022	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/January-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

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/January-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/January-2022	H-MED-MT68-210122/269
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	H-MED-MT68-210122/270
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	https://corp.mediatek.com/product-security-bulletin/January-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**		
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/January-2022	H-MED-MT68-210122/272
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/January-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/January-2022	H-MED-MT68-210122/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05917620. **CVE ID : CVE-2022-20019**		
mt6893					
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/January-2022	H-MED-MT68-210122/275
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-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/January-2022	H-MED-MT68-210122/277

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/January-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/January-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/January-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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			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**	bulletin/January-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/January-2022	H-MED-MT68-210122/282
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/January-2022	H-MED-MT68-210122/283
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	https://corp.mediatek.com/product-security-bulletin/Janu	H-MED-MT76-210122/284

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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT76-210122/286

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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT76-210122/289

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/January-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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT76-210122/291
Missing	04-Jan-22	3.3	In Bluetooth, there is a	https://corp.	H-MED-

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/January-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/January-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/January-2022	H-MED-MT79-210122/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20023		
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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT79-210122/295
mt7922					
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/January-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/January-2022	H-MED-MT81-210122/297

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/January-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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT81-210122/300

Weakness	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**		
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/January-2022	H-MED-MT81-210122/301
mt8167					
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/January-2022	H-MED-MT81-210122/302
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-MT81-210122/303

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/January-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/January-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/January-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

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. **CVE ID : CVE-2022-20022**	bulletin/January-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/January-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/January-2022	H-MED-MT81-210122/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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/January-2022	H-MED-MT81-210122/309
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/January-2022	H-MED-MT81-210122/310
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	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT81-210122/311

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/January-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/January-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/January-2022	H-MED-MT81-210122/314

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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT81-210122/315
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/January-2022	H-MED-MT81-210122/316
mt8173					
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/January-2022	H-MED-MT81-210122/317

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. **CVE ID : CVE-2022-20018**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT81-210122/318
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/January-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/January-2022	H-MED-MT81-210122/320

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/January-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/January-2022	H-MED-MT81-210122/322
mt8175					
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/January-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					
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/January-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/January-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/January-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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	H-MED-MT81-210122/328
mt8185					
Concurrent	04-Jan-22	4.4	In vow driver, there is a	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			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**	mediatek.com/product-security-bulletin/January-2022	MT81-210122/329
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/January-2022	H-MED-MT81-210122/330
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/January-2022	H-MED-MT81-210122/331
Improper Restriction of Operations within the Bounds of a	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	https://corp.mediatek.com/product-security-bulletin/January-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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT81-210122/333
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. **CVE ID : CVE-2022-20012**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT81-210122/334
mt8195					
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

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. Patch ID: ALPS06198608; Issue ID: ALPS06198608. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	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/January-2022	H-MED-MT83-210122/337
Improper Restriction of Operations within the Bounds of a	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	https://corp.mediatek.com/product-security-bulletin/January-2022	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. **CVE ID : CVE-2022-20021**	https://corp.mediatek.com/product-security-bulletin/January-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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT83-210122/340
Missing Release of	04-Jan-22	3.3	In Bluetooth, there is a possible application crash	https://corp.mediatek.com	H-MED-MT83-

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/January-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/January-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/January-2022	H-MED-MT83-210122/343
Improper Restriction of	04-Jan-22	2.1	In libvcodecdrv, there is a possible information disclosure due to a missing	https://corp.mediatek.com/product-	H-MED-MT83-210122/344

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/January-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/January-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/January-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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT83-210122/347
mt8362b					
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/January-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/January-2022	H-MED-MT83-210122/349

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. **CVE ID : CVE-2022-20023**	https://corp.mediatek.com/product-security-bulletin/January-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/January-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/January-2022	H-MED-MT83-210122/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018. **CVE ID : CVE-2022-20018**		
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/January-2022	H-MED-MT83-210122/353
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/January-2022	H-MED-MT83-210122/354
mt8385					
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	https://corp.mediatek.com/product-security-bulletin/January-2022	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. **CVE ID : CVE-2022-20014**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT83-210122/356
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/January-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/January-2022	H-MED-MT83-210122/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT83-210122/359
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/January-2022	H-MED-MT83-210122/360
mt8765					
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	https://corp.mediatek.com/product-security-	H-MED-MT87-210122/361

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/January-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/January-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/January-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

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. **CVE ID : CVE-2022-20022**	bulletin/January-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/January-2022	H-MED-MT87-210122/365
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. **CVE ID : CVE-2022-20020**	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT87-210122/366
Missing	04-Jan-22	3.3	In Bluetooth, there is a	https://corp.	H-MED-

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/January-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/January-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/January-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-

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/January-2022	210122/370
mt8786					
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/January-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/January-2022	H-MED-MT87-210122/372
mt8788					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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/January-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/January-2022	H-MED-MT87-210122/374
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/January-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/January-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/January-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/January-2022	H-MED-MT87-210122/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20023		
mt8789					
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-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/January-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/January-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-

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/January-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/January-2022	H-MED-MT87-210122/383
mt8791					
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-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	Description & CVE ID	Patch	NCIIPC ID
			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**	bulletin/January-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/January-2022	H-MED-MT87-210122/386
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/January-2022	H-MED-MT87-210122/387
mt8797					
Concurrent Execution using Shared Resource with Improper	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.	https://corp.mediatek.com/product-security-bulletin/January-2022	H-MED-MT87-210122/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('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/January-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/January-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/January-2022	H-MED-MT87-210122/391

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://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=1	H-SAM-EXYN-210122/392
Operating System					
alpinelinux					
alpine_linux					
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.org/alpine/aports/-/issues/13368	O-ALP-ALPI-210122/393
Debian					
debian_linux					
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	https://redmine.lighttpd.net/issues/3134	O-DEB-DEBI-210122/394

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 Neutralization 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://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84, https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/, https://github.com/WordPress/wordpress-develop/commit/17efac8c8ec64555eff5cf51a3eff81e06317214	O-DEB-DEBI-210122/395
Improper Neutralization 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. Low-privileged authenticated users (like author) in	https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/, https://githu	O-DEB-DEBI-210122/396

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/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w	
Improper Neutralization 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. **CVE ID : CVE-2022-21663**	https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/, https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-332h	O-DEB-DEBI-210122/397
Improper Neutralization 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://wordpress.org/news/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**	https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-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://security.samsungmobile.com/securityUpdate.smsb?year=2022&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://security.samsungmobile.com/securityUpdate.smsb?year=2022&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://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=1	O-GOO-ANDR-210122/401
Improper	10-Jan-22	2.1	(Applicable to China models	https://secur	O-GOO-

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.samsungmobile.com/securityUpdate.smsb?year=2022&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://security.samsungmobile.com/securityUpdate.smsb?year=2022&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://security.samsungmobile.com/securityUpdate.smsb?year=2022&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://security.samsungmobile.com/securityUpdate.smsb?year=2022&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://security.samsungmobile.com/securityUpdate.smsb?year=20	O-GOO-ANDR-210122/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2022-22270**	22&month=1	
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://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=1	O-GOO-ANDR-210122/407
Incorrect Authorization	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_STATE permission **CVE ID : CVE-2022-22272**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=1	O-GOO-ANDR-210122/408
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/January-2022	O-GOO-ANDR-210122/409
Concurrent Execution using Shared Resource with Improper Synchronization ('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/January-2022	O-GOO-ANDR-210122/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05837742. **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/January-2022	O-GOO-ANDR-210122/411
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/January-2022	O-GOO-ANDR-210122/412
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/January-2022	O-GOO-ANDR-210122/413
Use of Uninitialized	04-Jan-22	2.1	In seninf driver, there is a possible information	https://corp.mediatek.com	O-GOO-ANDR-

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/January-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/January-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/January-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

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. **CVE ID : CVE-2022-20022**	https://corp.mediatek.com/product-security-bulletin/January-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/January-2022	O-GOO-ANDR-210122/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Microsoft					
windows_10					
Improper Privilege Management	11-Jan-22	7.2	Virtual Machine IDE Drive Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21833**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21833	O-MIC-WIND-210122/420
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21834	O-MIC-WIND-210122/421
Improper Privilege Management	11-Jan-22	7.2	Microsoft Cryptographic Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21835**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21835	O-MIC-WIND-210122/422
Improper Certificate Validation	11-Jan-22	7.2	Windows Certificate Spoofing Vulnerability. **CVE ID : CVE-2022-21836**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21836	O-MIC-WIND-210122/423
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21838	O-MIC-WIND-210122/424
Uncontrolled Resource	11-Jan-22	2.1	Windows Event Tracing Discretionary Access Control	https://portal.msrc.micros	O-MIC-WIND-

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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21849	O-MIC-WIND-210122/429
N/A	11-Jan-22	9.3	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210122/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21833	guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21843	O-MIC-WIND-210122/446

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.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/advisory/CVE-2022-21852	
Improper Privilege Management	11-Jan-22	9	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21857**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-210122/457

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21835	O-MIC-WIND-210122/459
Improper Certificate Validation	11-Jan-22	7.2	Windows Certificate Spoofing Vulnerability. **CVE ID : CVE-2022-21836**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21843	O-MIC-WIND-210122/462
Uncontrolled Resource	11-Jan-22	7.1	Windows IKE Extension Denial of Service	https://portal.msrc.micros	O-MIC-WIND-

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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/adv	O-MIC-WIND-210122/468

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21838	O-MIC-WIND-210122/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21843	O-MIC-WIND-210122/474
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21848	O-MIC-WIND-210122/475
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21850	O-MIC-WIND-210122/476
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21851	O-MIC-WIND-210122/477
Improper Privilege Management	11-Jan-22	9	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21857**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21857	O-MIC-WIND-210122/478
Improper Privilege	11-Jan-22	6.9	Windows Accounts Control Elevation of Privilege	https://portal.msrc.micros	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. **CVE ID : CVE-2022-21859**	oft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21868	O-MIC-WIND-210122/482
windows_server					
Improper Privilege Management	11-Jan-22	7.2	Virtual Machine IDE Drive Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21833**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/adv	O-MIC-WIND-210122/484

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21852	O-MIC-WIND-210122/494
Improper Privilege Management	11-Jan-22	9	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21863	O-MIC-WIND-210122/500

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21868	O-MIC-WIND-210122/502
windows_server_2008					
Improper Privilege Management	11-Jan-22	7.2	Virtual Machine IDE Drive Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21833**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21835	O-MIC-WIND-210122/505
Improper Certificate Validation	11-Jan-22	7.2	Windows Certificate Spoofing Vulnerability.	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-210122/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21836	US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21850	O-MIC-WIND-210122/510
N/A	11-Jan-22	9.3	Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21862	O-MIC-WIND-210122/513
windows_server_2012					
Improper Privilege Management	11-Jan-22	7.2	Virtual Machine IDE Drive Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21833**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21835	O-MIC-WIND-210122/516

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21850	O-MIC-WIND-210122/521
N/A	11-Jan-22	9.3	Remote Desktop Client Remote Code Execution	https://portal.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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-210122/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2022-21868	
windows_server_2016					
Improper Privilege Management	11-Jan-22	7.2	Virtual Machine IDE Drive Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21833**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21833	O-MIC-WIND-210122/528
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21834	O-MIC-WIND-210122/529
Improper Privilege Management	11-Jan-22	7.2	Microsoft Cryptographic Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21835**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21835	O-MIC-WIND-210122/530
Improper Certificate Validation	11-Jan-22	7.2	Windows Certificate Spoofing Vulnerability. **CVE ID : CVE-2022-21836**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21836	O-MIC-WIND-210122/531
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21838	O-MIC-WIND-210122/532
Uncontrolled Resource	11-Jan-22	4.3	Windows IKE Extension Denial of Service	https://portal.msrc.micros	O-MIC-WIND-

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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21851	O-MIC-WIND-210122/537
Improper Privilege Management	11-Jan-22	9	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.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/advisory/CVE-2022-21857	
Improper Privilege Management	11-Jan-22	6.9	Windows Accounts Control Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21859**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21868	O-MIC-WIND-210122/543
windows_server_2019					

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-210122/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21839	guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-	O-MIC-WIND-210122/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21861	US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21868	O-MIC-WIND-210122/564