Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Acronis					
agent					
Incorrect Default Permissions	04-Feb-22	4.6	Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 **CVE ID : CVE-2022-24113**	https://security-advisory.acronis.com/advisories/SEC-2881	A-ACR-AGEN-170222/1
cyber_protect					
Incorrect Default Permissions	04-Feb-22	4.6	Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 **CVE ID : CVE-2022-24113**	https://security-advisory.acronis.com/advisories/SEC-2881	A-ACR-CYBE-170222/2
cyber_protect_home_office					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	04-Feb-22	4.6	Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 **CVE ID : CVE-2022-24113**	https://security-advisory.acronis.com/advisories/SEC-2881	A-ACR-CYBE-170222/3
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Feb-22	4.4	Local privilege escalation due to race condition on application startup. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 **CVE ID : CVE-2022-24114**	https://security-advisory.acronis.com/advisories/SEC-3316	A-ACR-CYBE-170222/4
Improper Verification of Cryptographic Signature	04-Feb-22	4.6	Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 **CVE ID : CVE-2022-24115**	https://security-advisory.acronis.com/advisories/SEC-3359	A-ACR-CYBE-170222/5
true_image					
Incorrect Default Permissions	04-Feb-22	4.6	Local privilege escalation due to excessive permissions assigned to child processes. The following products are	https://security-advisory.acronis.com/ad	A-ACR-TRUE-170222/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 **CVE ID : CVE-2022-24113**	visories/SEC-2881	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Feb-22	4.4	Local privilege escalation due to race condition on application startup. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 **CVE ID : CVE-2022-24114**	https://security-advisory.acronis.com/advisories/SEC-3316	A-ACR-TRUE-170222/7
Improper Verification of Cryptographic Signature	04-Feb-22	4.6	Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 **CVE ID : CVE-2022-24115**	https://security-advisory.acronis.com/advisories/SEC-3359	A-ACR-TRUE-170222/8
Apache					
activemq_artemis					
Uncontrolled Resource Consumption	04-Feb-22	5	In Apache ActiveMQ Artemis prior to 2.20.0 or 2.19.1, an attacker could partially disrupt availability (DoS) through uncontrolled resource consumption of	N/A	A-APA-ACTI-170222/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory. **CVE ID : CVE-2022-23913**		
james					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Feb-22	4	Fix of CVE-2021-40525 do not prepend delimiters upon valid directory validations. Affected implementations include: - maildir mailbox store - Sieve file repository This enables a user to access other users data stores (limited to user names being prefixed by the value of the username being used). **CVE ID : CVE-2022-22931**	https://lists.apache.org/thread/bp8yql4wws56jlh0vxoowj7foothsmpr	A-APA-JAME-170222/10
traffic_control					
Server-Side Request Forgery (SSRF)	06-Feb-22	5	In Apache Traffic Control Traffic Ops prior to 6.1.0 or 5.1.6, an unprivileged user who can reach Traffic Ops over HTTPS can send a specially-crafted POST request to /user/login/oauth to scan a port of a server that Traffic Ops can reach. **CVE ID : CVE-2022-23206**	https://lists.apache.org/thread/lsrd2mqj29vrvwsh8g0d560vvz8n126f	A-APA-TRAF-170222/11
beanstalk_console_project					
beanstalk_console					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Feb-22	4.3	Cross-site Scripting (XSS) - Reflected in Packagist ptrofimov/beanstalk_console prior to 1.7.12. **CVE ID : CVE-2022-0501**	https://github.com/ptrofimov/beanstalk_console/commit/e351c8260ec1d3718d9e475ee57c7e12c47f19da, https://hunt	A-BEA-BEAN-170222/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				r.dev/bounties/9af1c35e-3f74-4c93-a241-e8be01335ec7	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist ptrofimov/beanstalk_console prior to 1.7.14. **CVE ID : CVE-2022-0539**	https://hunter.dev/bounties/5f41b182-dda2-4c6f-9668-2a9afaed53af, https://github.com/ptrofimov/beanstalk_console/commit/5aea5f912f6e6d19dedb1fdfc25a29a2e1fc1694	A-BEA-BEAN-170222/13
blitzjs					
superjson					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	09-Feb-22	7.5	superjson is a program to allow JavaScript expressions to be serialized to a superset of JSON. In versions prior to 1.8.1 superjson allows input to run arbitrary code on any server using superjson input without prior authentication or knowledge. The only requirement is that the server implements at least one endpoint which uses superjson during request processing. This has been patched in superjson 1.8.1. Users are advised to update.	https://github.com/blitz-js/superjson/security/advisories/GHSA-5888-ffcr-r425	A-BLI-SUPE-170222/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds for this issue. **CVE ID : CVE-2022-23631**		
blog_project					
blog					
Unrestricted Upload of File with Dangerous Type	08-Feb-22	6.5	m1k1o/blog is a lightweight self-hosted facebook-styled PHP blog. Errors from functions `imagecreatefrom*` and `image*` have not been checked properly. Although PHP issued warnings and the upload function returned `false`, the original file (that could contain a malicious payload) was kept on the disk. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-23626**	https://github.com/m1k1o/blog/security/advisories/GHSA-wmqj-5v54-24x4, https://github.com/m1k1o/blog/commit/6f5e59f1401c4a3cf2e518aa85b231ea14e8a2ef	A-BLO-BLOG-170222/15
Broadcom					
ca_harvest_software_change_manager					
Improper Neutralization of Formula Elements in a CSV File	04-Feb-22	6.5	CA Harvest Software Change Manager versions 13.0.3, 13.0.4, 14.0.0, and 14.0.1, contain a vulnerability in the CSV export functionality, due to insufficient input validation, that can allow a privileged user to potentially execute arbitrary code or commands. **CVE ID : CVE-2022-22689**	https://support.broadcom.com/security-advisory/content/security-advisories/CA20220203-01-Security-Notice-for-CA-Harvest-Software-Change-Manager/ES	A-BRO-CA_H-170222/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				DSA20297	
capsule8					
capsule8					
Improper Authentication	02-Feb-22	6.5	An authenticated and authorized agent user could potentially gain administrative access via an SQLi vulnerability to Capsule8 Console between versions 4.6.0 and 4.9.1. **CVE ID : CVE-2022-0366**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20220201-cap8-console-sqli	A-CAP-CAPS-170222/17
chatwoot					
chatwoot					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-22	4.3	Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0. **CVE ID : CVE-2022-0526**	https://huntr.dev/bounties/d8f5ce74-2a00-4813-b220-70af771b0edd, https://github.com/chatwoot/chatwoot/commit/9f37a6e2ba7a7212bb419e318b8061f472e82d9f	A-CHA-CHAT-170222/18
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-22	4.3	Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0. **CVE ID : CVE-2022-0527**	https://github.com/chatwoot/chatwoot/commit/a737f89c473e64f9abdf8ff13a3e64edefa28877, https://huntr.dev/bounti	A-CHA-CHAT-170222/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es/a2f598f6-c142-449a-96f8-b4b2f7a9e228	
Citrix					
workspace					
Incorrect Authorization	09-Feb-22	4.6	An Improper Access Control vulnerability exists in Citrix Workspace App for Linux 2012 - 2111 with App Protection installed that can allow an attacker to perform local privilege escalation. **CVE ID : CVE-2022-21825**	https://support.citrix.com/article/CTX338435	A-CIT-WORK-170222/20
codemiq					
wordpress_email_template_designer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-22	4.3	The WP HTML Mail WordPress plugin is vulnerable to unauthorized access which allows unauthenticated attackers to retrieve and modify theme settings due to a missing capability check on the /themesettings REST-API endpoint found in the ~/includes/class-template-designer.php file, in versions up to and including 3.0.9. This makes it possible for attackers with no privileges to execute the endpoint and add malicious JavaScript to a vulnerable WordPress site. **CVE ID : CVE-2022-0218**	https://plugins.trac.wordpress.org/changeset/2656984/wp-html-mail/trunk/includes/class-template-designer.php	A-COD-WORD-170222/21
Codesys					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
profinet					
NULL Pointer Dereference	02-Feb-22	5	Codesys Profinet in version V4.2.0.0 is prone to null pointer dereference that allows a denial of service (DoS) attack of an unauthenticated user via SNMP. **CVE ID : CVE-2022-22510**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17020&token=9acf91a2b5e1719ff71a019e86c3e8e411bfd252&download=	A-COD-PROF-170222/22
csv\\+_project					
csv\\+					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	6.8	Cross-site scripting vulnerability in CSV+ prior to 0.8.1 allows a remote unauthenticated attacker to inject an arbitrary script or an arbitrary OS command via a specially crafted CSV file that contains HTML a tag. **CVE ID : CVE-2022-21241**	N/A	A-CSV-CSV\-170222/23
dataease_project					
dataease					
Exposure of Resource to Wrong Sphere	08-Feb-22	6.5	In DataEase v1.6.1, an authenticated user can gain unauthorized access to all user information and can change the administrator password. **CVE ID : CVE-2022-23331**	N/A	A-DAT-DATA-170222/24
Djangoproject					
django					
Loop with Unreachable Exit	03-Feb-22	5	An issue was discovered in MultiPartParser in Django 2.2 before 2.2.27, 3.2 before	https://docs.djangoproject.com/en/4.0	A-DJA-DJAN-170222/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			3.2.12, and 4.0 before 4.0.2. Passing certain inputs to multipart forms could result in an infinite loop when parsing files. **CVE ID : CVE-2022-23833**	/releases/security/, https://www.djangoproject.com/weblog/2022/feb/01/security-releases/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-22	4.3	The {% debug %} template tag in Django 2.2 before 2.2.27, 3.2 before 3.2.12, and 4.0 before 4.0.2 does not properly encode the current context. This may lead to XSS. **CVE ID : CVE-2022-22818**	https://docs.djangoproject.com/en/4.0/releases/security/, https://www.djangoproject.com/weblog/2022/feb/01/security-releases/	A-DJA-DJAN-170222/26
Docker					
docker_desktop					
N/A	01-Feb-22	5	Docker Desktop before 4.4.4 on Windows allows attackers to move arbitrary files. **CVE ID : CVE-2022-23774**	https://docs.docker.com/docker-for-windows/release-notes/	A-DOC-DOCK-170222/27
Dounokouno					
transmitmail					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Feb-22	5	Directory traversal vulnerability in TransmitMail 2.5.0 to 2.6.1 allows a remote unauthenticated attacker to obtain an arbitrary file on the server via unspecified vectors. **CVE ID : CVE-2022-21193**	https://dounokouno.com/2022/01/25/about-the-vulnerability-of-transmitmail-v2-5-0-v2-6-1/	A-DOU-TRAN-170222/28
Improper	08-Feb-22	4.3	Cross-site scripting	https://doun	A-DOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in TransmitMail 2.5.0 to 2.6.1 allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-22146**	okouno.com/2022/01/25/about-the-vulnerability-of-transmitmail-v2-5-0-v2-6-1/	TRAN-170222/29
econosys-system					
php_mailform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	4.3	Reflected cross-site scripting vulnerability in the attached file name of php_mailform versions prior to Version 1.40 allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-21805**	N/A	A-ECO-PHP_-170222/30
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	4.3	Reflected cross-site scripting vulnerability in the checkbox of php_mailform versions prior to Version 1.40 allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-22142**	N/A	A-ECO-PHP_-170222/31
element					
desktop					
Use After Free	01-Feb-22	5.1	Element Desktop is a Matrix client for desktop platforms with Element Web at its core. Element Desktop before 1.9.7 is vulnerable to a remote program execution bug with user interaction. The exploit is non-trivial and requires clicking on a malicious link,	https://github.com/vector-im/element-desktop/security/advisories/GHSA-mjrg-9f8r-h3m7, https://githu	A-ELE-DESK-170222/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			followed by another button click. To the best of our knowledge, the vulnerability has never been exploited in the wild. If you are using Element Desktop < 1.9.7, we recommend upgrading at your earliest convenience. If successfully exploited, the vulnerability allows an attacker to specify a file path of a binary on the victim's computer which then gets executed. Notably, the attacker does *not* have the ability to specify program arguments. However, in certain unspecified configurations, the attacker may be able to specify an URI instead of a file path which then gets handled using standard platform mechanisms. These may allow exploiting further vulnerabilities in those mechanisms, potentially leading to arbitrary code execution. **CVE ID : CVE-2022-23597**	b.com/vector-im/element-desktop/commit/89b1e39b801655e595337708d4319ba4313feafa	
Elitecms					
elite_cms					
N/A	01-Feb-22	6.4	An issue in /admin/delete_image.php of eliteCMS v1.0 allows attackers to delete arbitrary files. **CVE ID : CVE-2022-24218**	N/A	A-ELI-ELIT-170222/33
Improper	01-Feb-22	7.5	eliteCMS v1.0 was discovered	N/A	A-ELI-ELIT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			to contain a SQL injection vulnerability via /admin/edit_page.php. **CVE ID : CVE-2022-24219**		170222/34
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Feb-22	7.5	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_post.php. **CVE ID : CVE-2022-24220**	N/A	A-ELI-ELIT-170222/35
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Feb-22	7.5	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/functions/functions.php. **CVE ID : CVE-2022-24221**	N/A	A-ELI-ELIT-170222/36
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Feb-22	7.5	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_user.php. **CVE ID : CVE-2022-24222**	N/A	A-ELI-ELIT-170222/37
embed_swagger_project					
embed_swagger					
Improper Neutralizatio	04-Feb-22	4.3	The Embed Swagger WordPress plugin is	N/A	A-EMB-EMBE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			vulnerable to Reflected Cross-Site Scripting due to insufficient escaping/sanitization and validation via the url parameter found in the ~/swagger-iframe.php file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 1.0.0. **CVE ID : CVE-2022-0381**		170222/38
emlog					
emlog					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-22	7.5	Emlog v6.0 was discovered to contain a SQL injection vulnerability via the $TagID parameter of getblogidsfromtagid(). **CVE ID : CVE-2022-23379**	N/A	A-EML-EMLO-170222/39
fleetdm					
fleet					
Improper Authentication	04-Feb-22	3.5	fleet is an open source device management, built on osquery. Versions prior to 4.9.1 expose a limited ability to spoof SAML authentication with missing audience verification. This impacts deployments using SAML SSO in two specific cases: 1. A malicious or compromised Service Provider (SP) could reuse the SAML response to log into Fleet as a user -- only if the user has an account	https://github.com/fleetdm/fleet/commit/35d5a7b285f15ddd47486fa656e8b1acf3d48374, https://github.com/fleetdm/fleet/security/advisories/GHSA-ch68-7cf4-	A-FLE-FLEE-170222/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with the same email in Fleet, _and_ the user signs into the malicious SP via SAML SSO from the same Identity Provider (IdP) configured with Fleet. 2. A user with an account in Fleet could reuse a SAML response intended for another SP to log into Fleet. This is only a concern if the user is blocked from Fleet in the IdP, but continues to have an account in Fleet. If the user is blocked from the IdP entirely, this cannot be exploited. Fleet 4.9.1 resolves this issue. Users unable to upgrade should: Reduce the length of sessions on your IdP to reduce the window for malicious re-use, Limit the amount of SAML Service Providers/Applications used by user accounts with access to Fleet, and When removing access to Fleet in the IdP, delete the Fleet user from Fleet as well. **CVE ID : CVE-2022-23600**	35vr	
follow-redirects_project					
follow-redirects					
Exposure of Sensitive Information to an Unauthorized Actor	09-Feb-22	4.3	Exposure of Sensitive Information to an Unauthorized Actor in NPM follow-redirects prior to 1.14.8. **CVE ID : CVE-2022-0536**	https://hunter.dev/bounties/7cf2bf90-52da-4d59-8028-a73b132de0db, https://github.com/follow	A-FOL-FOLL-170222/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				-redirects/follow-redirects/commit/62e546a99c07c3ee5e4e0718c84a6ca127c5c445	
fotobook_project					
fotobook					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-22	4.3	The Fotobook WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping and the use of $_SERVER['PHP_SELF'] found in the ~/options-fotobook.php file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 3.2.3. **CVE ID : CVE-2022-0380**	N/A	A-FOT-FOTO-170222/42
Foxit					
pdf_reader					
Out-of-bounds Write	04-Feb-22	6.8	A memory corruption vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.1.0.52543. A specially-crafted PDF document can trigger an exception which is improperly handled, leaving the engine in an invalid state, which can lead to memory corruption and arbitrary code execution. An attacker needs	N/A	A-FOX-PDF_-170222/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2022-22150**		
framasoft					
peertube					
Server-Side Request Forgery (SSRF)	08-Feb-22	5	Server-Side Request Forgery (SSRF) in GitHub repository chocobozzz/peertube prior to f33e515991a32885622b217bf2ed1d1b0d9d6832 **CVE ID : CVE-2022-0508**	https://github.com/chocobozzz/peertube/commit/f33e515991a32885622b217bf2ed1d1b0d9d6832, https://hunter.dev/bounties/c3724574-b6c9-430b-849b-40dd2b20f23c	A-FRA-PEER-170222/44
frourio					
frourio					
Improper Input Validation	07-Feb-22	6.5	Frourio is a full stack framework, for TypeScript. Frourio users who uses frourio version prior to v0.26.0 and integration with class-validator through `validators/` folder are subject to a input validation vulnerability. Validators do not work properly for request bodies and queries in specific situations and some input is	https://github.com/frourio/frourio/security/advisories/GHSA-8xxm-h73r-ghfj, https://github.com/frourio/frourio/commit/7c19ac5363305b	A-FRO-FROU-170222/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not validated at all. Users are advised to update frourio to v0.26.0 or later and to install `class-transformer` and `reflect-metadata`. **CVE ID : CVE-2022-23623**	81b1c6b5232620228763d427af	
frourio-express					
Improper Input Validation	07-Feb-22	6.5	Frourio-express is a minimal full stack framework, for TypeScript. Frourio-express users who uses frourio-express version prior to v0.26.0 and integration with class-validator through `validators/` folder are subject to a input validation vulnerability. Validators do not work properly for request bodies and queries in specific situations and some input is not validated at all. Users are advised to update frourio to v0.26.0 or later and to install `class-transformer` and `reflect-metadata`. **CVE ID : CVE-2022-23624**	https://github.com/frouriojs/frourio-express/commit/73ded5c6f9f1c126c0cb2d05c0505e9e4db142d2, https://github.com/frouriojs/frourio-express/security/advisories/GHSA-mmj4-777p-fpq9	A-FRO-FROU-170222/46
gibbonedu					
gibbon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-22	3.5	Multiple cross-site scripting (XSS) vulnerabilities in the component outcomes_addProcess.php of Gibbon CMS v22.0.01 allow attackers to execute arbitrary web scripts or HTML via a crafted payload insterted into the name, category, description parameters.	N/A	A-GIB-GIBB-170222/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23871		
gin-vue-admin_project					
gin-vue-admin					
Missing Authorization	09-Feb-22	5.5	Gin-vue-admin is a backstage management system based on vue and gin. In versions prior to 2.4.7 low privilege users are able to modify higher privilege users. Authentication is missing on the `setUserInfo` function. Users are advised to update as soon as possible. There are no known workarounds. **CVE ID : CVE-2022-21660**	https://github.com/flipped-aurora/gin-vue-admin/security/advisories/GHSA-xxvh-9c87-pqjx	A-GIN-GIN--170222/48
Github					
gh-ost					
Improper Input Validation	01-Feb-22	4.3	gh-ost is a triggerless online schema migration solution for MySQL. Versions prior to 1.1.3 are subject to an arbitrary file read vulnerability. The attacker must have access to the target host or trick an administrator into executing a malicious gh-ost command on a host running gh-ost, plus network access from host running gh-ost to the attack's malicious MySQL server. The `-database` parameter does not properly sanitize user input which can lead to arbitrary file reads. **CVE ID : CVE-2022-21687**	https://github.com/github/gh-ost/commit/a91ab042de013cfd8fbb63376343893 2d9080d8f, https://github.com/github/gh-ost/security/advisories/GHSA-rrp4-2xx3-mv29	A-GIT-GH-O-170222/49
Google					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
go-attestation					
Improper Input Validation	04-Feb-22	2.1	An improper input validation vulnerability in go-attestation before 0.3.3 allows local users to provide a maliciously-formed Quote over no/some PCRs, causing AKPublic.Verify to succeed despite the inconsistency. Subsequent use of the same set of PCR values in Eventlog.Verify lacks the authentication performed by quote verification, meaning a local attacker could couple this vulnerability with a maliciously-crafted TCG log in Eventlog.Verify to spoof events in the TCG log, hence defeating remotely-attested measured-boot. We recommend upgrading to Version 0.4.0 or above. **CVE ID : CVE-2022-0317**	N/A	A-GOO-GO-A-170222/50
tensorflow					
Divide By Zero	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would trigger a division by zero in `BiasAndClamp` implementation. There is no check that the `bias_size` is non zero. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in	https://github.com/tensorflow/tensorflow/commit/8c6f391a2282684a25cbfec7687bd5d35261a209, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gf2j-	A-GOO-TENS-170222/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2022-23557**	f278-xh4v	
Integer Overflow or Wraparound	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause an integer overflow in `TfLiteIntArrayCreate`. The `TfLiteIntArrayGetSizeInBytes` returns an `int` instead of a `size_t. An attacker can control model inputs such that `computed_size` overflows the size of `int` datatype. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23558**	https://github.com/tensorflow/tensorflow/commit/a1e1511dde36b3f8aa27a6ec630838e7ea40e091, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9gwq-6cwj-47h3	A-GOO-TENS-170222/52
Integer Overflow or Wraparound	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause an integer overflow in embedding lookup operations. Both `embedding_size` and `lookup_size` are products of values provided by the user. Hence, a malicious user could trigger overflows in the multiplication. In certain scenarios, this can then result in heap OOB read/write. Users are advised to upgrade	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-98p5-x8x4-c9m5, https://github.com/tensorflow/tensorflow/commit/a4e401da71458d253b05e41f28637	A-GOO-TENS-170222/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a patched version. **CVE ID : CVE-2022-23559**	b65baf64be4	
Out-of-bounds Read	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would allow limited reads and writes outside of arrays in TFLite. This exploits missing validation in the conversion from sparse tensors to dense tensors. The fix is included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2022-23560**	https://github.com/tensorflow/tensorflow/commit/6364463d6f5b6254cac3d6aedf999b6a96225038, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4hvf-hxvg-f67v	A-GOO-TENS-170222/54
Out-of-bounds Write	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause a write outside of bounds of an array in TFLite. In fact, the attacker can override the linked list used by the memory allocator. This can be leveraged for an arbitrary write primitive under certain conditions. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9c78-vcq7-7vxq, https://github.com/tensorflow/tensorflow/commit/6c0b2b70eeee588591680f5b7d5d38175fd7cdf6	A-GOO-TENS-170222/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are also affected and still in supported range. **CVE ID : CVE-2022-23561**		
Integer Overflow or Wraparound	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of `Range` suffers from integer overflows. These can trigger undefined behavior or, in some scenarios, extremely large allocations. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23562**	https://github.com/tensorflow/tensorflow/commit/f0147751fd5d2ff23251149ebad9af9f03010732, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qx3f-p745-w4hr	A-GOO-TENS-170222/56
Exposure of Resource to Wrong Sphere	04-Feb-22	3.3	Tensorflow is an Open Source Machine Learning Framework. In multiple places, TensorFlow uses `tempfile.mktemp` to create temporary files. While this is acceptable in testing, in utilities and libraries it is dangerous as a different process can create the file between the check for the filename in `mktemp` and the actual creation of the file by a subsequent operation (a TOC/TOU type of weakness). In several instances, TensorFlow was supposed to actually create a temporary directory instead of a file. This logic bug is hidden away	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wc4g-r73w-x8mm	A-GOO-TENS-170222/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by the `mktemp` function usage. We have patched the issue in several commits, replacing `mktemp` with the safer `mkstemp`/`mkdtemp` functions, according to the usage pattern. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2022-23563**		
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. When decoding a resource handle tensor from protobuf, a TensorFlow process can encounter cases where a `CHECK` assertion is invalidated based on user controlled arguments. This allows attackers to cause denial of services in TensorFlow processes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23564**	https://github.com/tensorflow/tensorflow/commit/14fea662350e7c26eb5fe1be2ac31704e5682ee6, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8rcj-c8pj-v3m3	A-GOO-TENS-170222/58
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. An attacker can trigger denial of service via assertion failure by altering a `SavedModel` on disk such that `AttrDef`s of some operation are duplicated. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/c2b31ff2d3151acb230edc3f5b1832d2c713a9e0, https://githu	A-GOO-TENS-170222/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23565**	b.com/tensorflow/tensorflow/security/advisories/GHSA-4v5p-v5h9-6xjx	
Out-of-bounds Write	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. TensorFlow is vulnerable to a heap OOB write in `Grappler`. The `set_output` function writes to an array at the specified index. Hence, this gives a malicious user a write primitive. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23566**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-5qw5-89mw-wcg2, https://github.com/tensorflow/tensorflow/commit/97282c6d0d34476b6ba033f961590b783fa184cd	A-GOO-TENS-170222/60
Integer Overflow or Wraparound	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementations of `Sparse*Cwise*` ops are vulnerable to integer overflows. These can be used to trigger large allocations (so, OOM based denial of service) or `CHECK`-fails when building new `TensorShape` objects (so, assert failures based denial of service). We are missing	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rrx2-r989-2c43, https://github.com/tensorflow/tensorflow/blob/master/tensorflow/security/advisory/tfs	A-GOO-TENS-170222/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some validation on the shapes of the input tensors as well as directly constructing a large `TensorShape` with user-provided dimensions. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23567**	a-2021-198.md	
Integer Overflow or Wraparound	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `AddManySparseToTensorsMap` is vulnerable to an integer overflow which results in a `CHECK`-fail when building new `TensorShape` objects (so, an assert failure based denial of service). We are missing some validation on the shapes of the input tensors as well as directly constructing a large `TensorShape` with user-provided dimensions. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23568**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6445-fm66-fvq2, https://github.com/tensorflow/tensorflow/commit/b51b82fe65ebace4475e3c54eb089c18a4403f1c	A-GOO-TENS-170222/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. Multiple operations in TensorFlow can be used to trigger a denial of service via `CHECK`-fails (i.e., assertion failures). This is similar to TFSA-2021-198 and has similar fixes. We have patched the reported issues in multiple GitHub commits. It is possible that other similar instances exist in TensorFlow, we will issue fixes as these are discovered. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23569**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qj5r-f9mv-rffh, https://github.com/tensorflow/tensorflow/blob/master/tensorflow/security/advisory/tfsa-2021-198.md	A-GOO-TENS-170222/63
NULL Pointer Dereference	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, TensorFlow might do a null-dereference if attributes of some mutable arguments to some operations are missing from the proto. This is guarded by a `DCHECK`. However, `DCHECK` is a no-op in production builds and an assertion failure in debug builds. In the first case execution proceeds to the dereferencing of the null	https://github.com/tensorflow/tensorflow/commit/8a513cec4bec15961fbfdedcaa5376522980455c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9p77-mmrw-69c7	A-GOO-TENS-170222/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer, whereas in the second case it results in a crash due to the assertion failure. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23570**		
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, a TensorFlow process can encounter cases where a `CHECK` assertion is invalidated based on user controlled arguments, if the tensors have an invalid `dtype` and 0 elements or an invalid shape. This allows attackers to cause denial of services in TensorFlow processes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23571**	https://github.com/tensorflow/tensorflow/commit/5b491cd5e41ad63735161cec9c2a568172c8b6a3, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j3mj-fhpq-qqjj	A-GOO-TENS-170222/65
Improper Check for Unusual or Exceptional Conditions	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, TensorFlow can fail to specialize a type during shape inference. This case is	https://github.com/tensorflow/tensorflow/commit/cb164786dc891ea11d3	A-GOO-TENS-170222/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			covered by the `DCHECK` function however, `DCHECK` is a no-op in production builds and an assertion failure in debug builds. In the first case execution proceeds to the `ValueOrDie` line. This results in an assertion failure as `ret` contains an error `Status`, not a value. In the second case we also get a crash due to the assertion failure. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23572**	a900e90367c339305dc7b, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rww7-2gpw-fv6j	
Use of Uninitialized Resource	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of `AssignOp` can result in copying uninitialized data to a new tensor. This later results in undefined behavior. The implementation has a check that the left hand side of the assignment is initialized (to minimize number of allocations), but does not check that the right hand side is also initialized. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q85f-69q7-55h2, https://github.com/tensorflow/tensorflow/commit/ef1d027be116f25e25bb94a60da491c2cf55bd0b	A-GOO-TENS-170222/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are also affected and still in supported range. **CVE ID : CVE-2022-23573**		
Out-of-bounds Read	04-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. There is a typo in TensorFlow's `SpecializeType` which results in heap OOB read/write. Due to a typo, `arg` is initialized to the `i`th mutable argument in a loop where the loop index is `j`. Hence it is possible to assign to `arg` from outside the vector of arguments. Since this is a mutable proto value, it allows both read and write to outside of bounds data. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23574**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-77gp-3h4r-6428, https://github.com/tensorflow/tensorflow/commit/0657c83d08845cc434175934c642299de2c0f042	A-GOO-TENS-170222/68
Integer Overflow or Wraparound	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `OpLevelCostEstimator::CalculateTensorSize` is vulnerable to an integer overflow if an attacker can create an operation which would involve a tensor with large enough number of elements. The fix will be included in TensorFlow 2.8.0. We will	https://github.com/tensorflow/tensorflow/commit/fcd18ce3101f245b083b30655c27b239dc72221e, https://github.com/tensorflow/tensorflow/security/advisories	A-GOO-TENS-170222/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23575**	/GHSA-c94w-c95p-phf8	
Integer Overflow or Wraparound	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `OpLevelCostEstimator::CalculateOutputSize` is vulnerable to an integer overflow if an attacker can create an operation which would involve tensors with large enough number of elements. We can have a large enough number of dimensions in `output_shape.dim()` or just a small number of dimensions being large enough to cause an overflow in the multiplication. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23576**	https://github.com/tensorflow/tensorflow/commit/b9bd6cfd1c50e6807846af9a86f9b83cafc9c8ae, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wm93-f238-7v37	A-GOO-TENS-170222/70
NULL Pointer Dereference	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `GetInitOp` is vulnerable to a crash caused by dereferencing a null pointer.	https://github.com/tensorflow/tensorflow/commit/4f38b1ac8e42727e18a2f0bde06d3be	A-GOO-TENS-170222/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23577**	e8e77b250, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8cxv-76p7-jxwr	
Missing Release of Memory after Effective Lifetime	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. If a graph node is invalid, TensorFlow can leak memory in the implementation of `ImmutableExecutorState::Initialize`. Here, we set `item->kernel` to `nullptr` but it is a simple `OpKernel*` pointer so the memory that was previously allocated to it would leak. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23578**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8r7c-3cm2-3h8f, https://github.com/tensorflow/tensorflow/commit/c79ccba517dbb1a0ccb9b01ee3bd2a63748b60dd	A-GOO-TENS-170222/72
Reachable Assertion	04-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a `SavedModel` such that `SafeToRemoveIdentity` would trigger `CHECK` failures. The fix will be	https://github.com/tensorflow/tensorflow/commit/92dba16749fae36c246bec3f9ba474d9ddeb7662, https://github.com/tenso	A-GOO-TENS-170222/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23579**	rflow/tensorflow/security/advisories/GHSA-5f2r-qp73-37mr	
Uncontrolled Resource Consumption	04-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. During shape inference, TensorFlow can allocate a large vector based on a value from a tensor controlled by the user. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23580**	https://github.com/tensorflow/tensorflow/commit/1361fb7e29449629e1df94d44e0427ebec8c83c7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-627q-g293-49q7	A-GOO-TENS-170222/74
Reachable Assertion	04-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a `SavedModel` such that `IsSimplifiableReshape` would trigger `CHECK` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fq86-3f29-px2c, https://github.com/tensorflow/tensorflow/commit/1fb27733f943295d874417630edd3b38b34ce082	A-GOO-TENS-170222/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2022-23581**		
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that `TensorByteSize` would trigger `CHECK` failures. `TensorShape` constructor throws a `CHECK`-fail if shape is partial or has a number of elements that would overflow the size of an `int`. The `PartialTensorShape` constructor instead does not cause a `CHECK`-abort if the shape is partial, which is exactly what this function needs to be able to return `-1`. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23582**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4j82-5ccr-4r8v, https://github.com/tensorflow/tensorflow/commit/c2426bba00a01de6913738df8fa78e0215fcce02	A-GOO-TENS-170222/76
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that any binary op would trigger `CHECK` failures. This occurs when the protobuf part corresponding to the tensor arguments is	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gjqc-q9g6-q2j3, https://github.com/tensorflow/tensor	A-GOO-TENS-170222/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modified such that the `dtype` no longer matches the `dtype` expected by the op. In that case, calling the templated binary operator for the binary op would receive corrupted data, due to the type confusion involved. If `Tin` and `Tout` don't match the type of data in `out` and `input_*` tensors then `flat<*>` would interpret it wrongly. In most cases, this would be a silent failure, but we have noticed scenarios where this results in a `CHECK` crash, hence a denial of service. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23583**	flow/commit/a7c02f1a9bbc35473969618a09ee5f9f5d3e52d9	
Use After Free	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a use after free behavior when decoding PNG images. After `png::CommonFreeDecode(&decode)` gets called, the values of `decode.width` and `decode.height` are in an unspecified state. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow	https://github.com/tensorflow/tensorflow/commit/e746adbfcfee15e9cfdb391ff746c765b99bdf9b, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-24x4-	A-GOO-TENS-170222/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23584**	6qmh-88qg	
Missing Release of Memory after Effective Lifetime	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. When decoding PNG images TensorFlow can produce a memory leak if the image is invalid. After calling `png::CommonInitDecode(..., &decode)`, the `decode` value contains allocated buffers which can only be freed by calling `png::CommonFreeDecode(&decode)`. However, several error case in the function implementation invoke the `OP_REQUIRES` macro which immediately terminates the execution of the function, without allowing for the memory free to occur. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23585**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fq6p-6334-8gr4, https://github.com/tensorflow/tensorflow/commit/ab51e5b813573dc9f51efa335aebcf2994125ee9	A-GOO-TENS-170222/79
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that assertions in	https://github.com/tensorflow/tensorflow/commit/3d89911481ba6ebe8c8	A-GOO-TENS-170222/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`function.cc` would be falsified and crash the Python interpreter. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23586**	8c1c0b595412121e6c645, https://github.com/tensorflow/tensorflow/commit/dcc21c7bc972b10b6fb95c2fb0f4ab5a59680ec2	
Integer Overflow or Wraparound	04-Feb-22	7.5	Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow is vulnerable to an integer overflow during cost estimation for crop and resize. Since the cropping parameters are user controlled, a malicious person can trigger undefined behavior. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23587**	https://github.com/tensorflow/tensorflow/commit/0aaaae6eca5a7175a193696383f582f53adab23f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8jj7-5vxc-pg2q	A-GOO-TENS-170222/81
Reachable Assertion	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that Grappler optimizer would attempt to build a tensor using a reference	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fx5c-h9f6-rv7c, https://githu	A-GOO-TENS-170222/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`dtype`. This would result in a crash due to a `CHECK`-fail in the `Tensor` constructor as reference types are not allowed. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23588**	b.com/tensorflow/tensorflow/commit/6b5adc0877de832b2a7c189532dbbbc64622eeb6	
NULL Pointer Dereference	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow can trigger a null pointer dereference. There are 2 places where this can occur, for the same malicious alteration of a `SavedModel` file (fixing the first one would trigger the same dereference in the second place). First, during constant folding, the `GraphDef` might not have the required nodes for the binary operation. If a node is missing, the correposning `mul_*child` would be null, and the dereference in the subsequent line would be incorrect. We have a similar issue during `IsIdentityConsumingSwitch`. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9px9-73fg-3fqp, https://github.com/tensorflow/tensorflow/commit/0a365c029e437be0349c31f8d4c9926b69fa3fa1	A-GOO-TENS-170222/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23589**		
Improper Check for Unusual or Exceptional Conditions	04-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. A `GraphDef` from a TensorFlow `SavedModel` can be maliciously altered to cause a TensorFlow process to crash due to encountering a `StatusOr` value that is an error and forcibly extracting the value from it. We have patched the issue in multiple GitHub commits and these will be included in TensorFlow 2.8.0 and TensorFlow 2.7.1, as both are affected. **CVE ID : CVE-2022-23590**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pqrv-8r2f-7278, https://github.com/tensorflow/tensorflow/commit/955059813cc325dc1db5e2daa6221271406d4439	A-GOO-TENS-170222/84
Uncontrolled Resource Consumption	04-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. The `GraphDef` format in TensorFlow does not allow self recursive functions. The runtime assumes that this invariant is satisfied. However, a `GraphDef` containing a fragment such as the following can be consumed when loading a `SavedModel`. This would result in a stack overflow during execution as resolving each `NodeDef` means resolving the function	https://github.com/tensorflow/tensorflow/commit/448a16182065bd08a202d9057dd8ca541e67996c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-247x-	A-GOO-TENS-170222/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			itself and its nodes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23591**	2f9f-5wp7	
Out-of-bounds Read	04-Feb-22	5.5	Tensorflow is an Open Source Machine Learning Framework. TensorFlow's type inference can cause a heap out of bounds read as the bounds checking is done in a `DCHECK` (which is a no-op during production). An attacker can control the `input_idx` variable such that `ix` would be larger than the number of values in `node_t.args`. The fix will be included in TensorFlow 2.8.0. This is the only affected version. **CVE ID : CVE-2022-23592**	https://github.com/tensorflow/tensorflow/commit/c99d98cd189839dcf51aee94e7437b54b31f8abd, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vq36-27g6-p492	A-GOO-TENS-170222/86
Improper Check for Unusual or Exceptional Conditions	04-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. The `simplifyBroadcast` function in the MLIR-TFRT infrastructure in TensorFlow is vulnerable to a segfault (hence, denial of service), if called with scalar shapes. If all shapes are scalar, then `maxRank` is 0, so we build an empty `SmallVector`. The fix will be included in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gwcx-jrx4-92w2, https://github.com/tensorflow/tensorflow/commit/35f0fabb4c178253a964	A-GOO-TENS-170222/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.0. This is the only affected version. **CVE ID : CVE-2022-23593**	d7aabdbb15c6a398b69a	
Out-of-bounds Read	04-Feb-22	2.1	Tensorflow is an Open Source Machine Learning Framework. The TFG dialect of TensorFlow (MLIR) makes several assumptions about the incoming `GraphDef` before converting it to the MLIR-based dialect. If an attacker changes the `SavedModel` format on disk to invalidate these assumptions and the `GraphDef` is then converted to MLIR-based IR then they can cause a crash in the Python interpreter. Under certain scenarios, heap OOB read/writes are possible. These issues have been discovered via fuzzing and it is possible that more weaknesses exist. We will patch them as they are discovered. **CVE ID : CVE-2022-23594**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9x52-887g-fhc2	A-GOO-TENS-170222/88
NULL Pointer Dereference	04-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. When building an XLA compilation cache, if default settings are used, TensorFlow triggers a null pointer dereference. In the default scenario, all devices are allowed, so `flr->config_proto` is `nullptr`. The fix will be included in TensorFlow 2.8.0. We will	https://github.com/tensorflow/tensorflow/commit/e21af685e1828f7ca65038307df5cc06de4479e8, https://github.com/tensorflow/tensorflow/securit	A-GOO-TENS-170222/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-23595**	y/advisories/GHSA-fpcp-9h7m-ffpx	
Divide By Zero	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The estimator for the cost of some convolution operations can be made to execute a division by 0. The function fails to check that the stride argument is strictly positive. Hence, the fix is to add a check for the stride argument to ensure it is valid. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21725**	https://github.com/tensorflow/tensorflow/commit/3218043d6d3a019756607643cf65574fbfef5d7a, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v3f7-j968-4h5f	A-GOO-TENS-170222/90
Out-of-bounds Read	03-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of `Dequantize` does not fully validate the value of `axis` and can result in heap OOB accesses. The `axis` argument can be `-1` (the default value for the optional argument) or any other positive value at most the number of	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-23hm-7w47-xw72, https://github.com/tensorflow/tensorflow/commit	A-GOO-TENS-170222/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dimensions of the input. Unfortunately, the upper bound is not checked and this results in reading past the end of the array containing the dimensions of the input tensor. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21726**	/23968a8bf65b009120c43b5ebcceaf52dbc9e943	
Integer Overflow or Wraparound	03-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of shape inference for `Dequantize` is vulnerable to an integer overflow weakness. The `axis` argument can be `-1` (the default value for the optional argument) or any other positive value at most the number of dimensions of the input. Unfortunately, the upper bound is not checked, and, since the code computes `axis + 1`, an attacker can trigger an integer overflow. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-c6fh-56w7-fvjw, https://github.com/tensorflow/tensorflow/commit/b64638ec5ccaa77b7c1eb90958e3d85ce381f91b	A-GOO-TENS-170222/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21727		
Out-of-bounds Read	03-Feb-22	5.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of shape inference for `ReverseSequence` does not fully validate the value of `batch_dim` and can result in a heap OOB read. There is a check to make sure the value of `batch_dim` does not go over the rank of the input, but there is no check for negative values. Negative dimensions are allowed in some cases to mimic Python's negative indexing (i.e., indexing from the end of the array), however if the value is too negative then the implementation of `Dim` would access elements before the start of an array. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21728**	https://github.com/tensorflow/tensorflow/commit/37c01fb5e25c3d8021306046019640 6c43d31995, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6gmv-pjp9-p8w8	A-GOO-TENS-170222/93
Integer Overflow or Wraparound	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `UnravelIndex` is vulnerable to a division by zero caused by an integer overflow bug.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-34f9-hjfq-rr8j,	A-GOO-TENS-170222/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21729**	https://github.com/tensorflow/tensorflow/commit/58b34c6c8250983948b5a781b426f6aa01fd47af	
Out-of-bounds Read	03-Feb-22	5.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of `FractionalAvgPoolGrad` does not consider cases where the input tensors are invalid allowing an attacker to read from outside of bounds of heap. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21730**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vjg4-v33c-ggc4, https://github.com/tensorflow/tensorflow/commit/002408c3696b173863228223d535f9de72a101a9	A-GOO-TENS-170222/95
Access of Resource Using Incompatible Type ('Type Confusion')	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of shape inference for `ConcatV2` can be used to trigger a denial of service attack via a segfault caused by a type confusion. The `axis` argument is translated into `concat_dim` in the `ConcatShapeHelper` helper function. Then, a value for `min_rank` is computed	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m4hf-j54p-p353, https://github.com/tensorflow/tensorflow/commit/08d7b00c0	A-GOO-TENS-170222/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based on `concat_dim`. This is then used to validate that the `values` tensor has at least the required rank. However, `WithRankAtLeast` receives the lower bound as a 64-bits value and then compares it against the maximum 32-bits integer value that could be represented. Due to the fact that `min_rank` is a 32-bits value and the value of `axis`, the `rank` argument is a negative value, so the error check is bypassed. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21731**	a5a2092636 3849f61172 9f53f3ec022	
Allocation of Resources Without Limits or Throttling	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `ThreadPoolHandle` can be used to trigger a denial of service attack by allocating too much memory. This is because the `num_threads` argument is only checked to not be negative, but there is no upper bound on its value. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and	https://github.com/tensorflow/tensorflow/commit/e3749a6d5d1e8d11806d4a2e9cc3123d1a90b75e, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-c582-c96p-r5cq	A-GOO-TENS-170222/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21732**		
Integer Overflow or Wraparound	03-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. The implementation of `StringNGrams` can be used to trigger a denial of service attack by causing an out of memory condition after an integer overflow. We are missing a validation on `pad_witdh` and that result in computing a negative value for `ngram_width` which is later used to allocate parts of the output. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21733**	https://github.com/tensorflow/tensorflow/commit/f68fdab93fb7f4ddb4eb438c8fe052753c9413e8, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-98j8-c9q4-r38g	A-GOO-TENS-170222/98
Access of Resource Using Incompatible Type ('Type Confusion')	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `MapStage` is vulnerable a `CHECK`-fail if the key tensor is not a scalar. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gcvh-66ff-4mwm, https://github.com/tensorflow/tensorflow/commit/f57315566d7094f322b	A-GOO-TENS-170222/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2022-21734**	784947093406c2aea0d7d	
Divide By Zero	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `FractionalMaxPool` can be made to crash a TensorFlow process via a division by 0. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21735**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-87v6-crgm-2gfj, https://github.com/tensorflow/tensorflow/commit/ba4e8ac4dc2991e350d5cc407f8598c8d4ee70fb	A-GOO-TENS-170222/100
NULL Pointer Dereference	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseTensorSliceDataset` has an undefined behavior: under certain condition it can be made to dereference a `nullptr` value. The 3 input arguments to `SparseTensorSliceDataset` represent a sparse tensor. However, there are some preconditions that these arguments must satisfy but these are not validated in the implementation. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pfjj-m3jj-9jc9, https://github.com/tensorflow/tensorflow/commit/965b97e4a9650495cda5a8c210ef6684b4b9eceb	A-GOO-TENS-170222/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21736**		
Improper Check for Unusual or Exceptional Conditions	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `*Bincount` operations allows malicious users to cause denial of service by passing in arguments which would trigger a `CHECK`-fail. There are several conditions that the input arguments must satisfy. Some are not caught during shape inference and others are not caught during kernel implementation. This results in `CHECK` failures later when the output tensors get allocated. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21737**	https://github.com/tensorflow/tensorflow/commit/7019ce4f68925fd01cdafde26f8d8c938f47e6f9, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f2vv-v9cg-qhh7	A-GOO-TENS-170222/102
Integer Overflow or Wraparound	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseCountSparseOutput` can be made to crash a TensorFlow process by an integer overflow whose result is then used in a memory allocation. The fix	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-x4qx-4fjv-hmw6, https://github.com/tensorflow/tensor	A-GOO-TENS-170222/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21738**	flow/commit/6f4d3e8139ec724dbbcb40505891c81dd1052c4a	
NULL Pointer Dereference	03-Feb-22	4	Tensorflow is an Open Source Machine Learning Framework. The implementation of `QuantizedMaxPool` has an undefined behavior where user controlled inputs can trigger a reference binding to null pointer. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21739**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-3mw4-6rj6-74g5, https://github.com/tensorflow/tensorflow/commit/53b0dd6dc5957652f35964af16b892ec9af4a559	A-GOO-TENS-170222/104
Out-of-bounds Write	03-Feb-22	6.5	Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseCountSparseOutput` is vulnerable to a heap overflow. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in	https://github.com/tensorflow/tensorflow/commit/2b7100d6cdff36aa21010a82269bc05a6d1cc74a, https://github.com/tensorflow/tensorflow/commit/adbbabdb0d3abb3cdeac	A-GOO-TENS-170222/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported range. **CVE ID : CVE-2022-21740**	69e38a96de1d678b24b3	
Divide By Zero	03-Feb-22	5	Tensorflow is an Open Source Machine Learning Framework. ### Impact An attacker can craft a TFLite model that would trigger a division by zero in the implementation of depthwise convolutions. The parameters of the convolution can be user controlled and are also used within a division operation to determine the size of the padding that needs to be added before applying the convolution. There is no check before this division that the divisor is strictly positive. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. **CVE ID : CVE-2022-21741**	https://github.com/tensorflow/tensorflow/commit/e5b0eec199c2d03de54fd6a7fd9275692218e2bc, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-428x-9xc2-m8mj	A-GOO-TENS-170222/106
gpac					
gpac					
NULL Pointer Dereference	04-Feb-22	4.3	A Null Pointer Dereference vulnerability exists in GPAC 1.1.0 via the xtra_box_write function in /box_code_base.c, which causes a Denial of Service. This vulnerability was fixed in commit 71f9871. **CVE ID : CVE-2022-24249**	N/A	A-GPA-GPAC-170222/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
grafana					
grafana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	2.1	Grafana is an open-source platform for monitoring and observability. In affected versions an attacker could serve HTML content thru the Grafana datasource or plugin proxy and trick a user to visit this HTML page using a specially crafted link and execute a Cross-site Scripting (XSS) attack. The attacker could either compromise an existing datasource for a specific Grafana instance or either set up its own public service and instruct anyone to set it up in their Grafana instance. To be impacted, all of the following must be applicable. For the data source proxy: A Grafana HTTP-based datasource configured with Server as Access Mode and a URL set, the attacker has to be in control of the HTTP server serving the URL of above datasource, and a specially crafted link pointing at the attacker controlled data source must be clicked on by an authenticated user. For the plugin proxy: A Grafana HTTP-based app plugin configured and enabled with a URL set, the attacker has to be in control of the HTTP server serving the URL of	https://github.com/grafana/grafana/security/advisories/GHSA-xc3p-28hw-q24g, https://grafana.com/blog/2022/02/08/grafana-7.5.15-and-8.3.5-released-with-moderate-severity-security-fixes/	A-GRA-GRAF-170222/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			above app, and a specially crafted link pointing at the attacker controlled plugin must be clocked on by an authenticated user. For the backend plugin resource: An attacker must be able to navigate an authenticated user to a compromised plugin through a crafted link. Users are advised to update to a patched version. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-21702**		
Cross-Site Request Forgery (CSRF)	08-Feb-22	6.8	Grafana is an open-source platform for monitoring and observability. Affected versions are subject to a cross site request forgery vulnerability which allows attackers to elevate their privileges by mounting cross-origin attacks against authenticated high-privilege Grafana users (for example, Editors or Admins). An attacker can exploit this vulnerability for privilege escalation by tricking an authenticated user into inviting the attacker as a new user with high privileges. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-21703**	https://github.com/grafana/grafana/pull/45083, https://grafana.com/blog/2022/02/08/grafana-7.5.15-and-8.3.5-released-with-moderate-severity-security-fixes/, https://github.com/grafana/grafana/security/advisories/GHSA-cmf4-h3xc-jw8w	A-GRA-GRAF-170222/109
Incorrect Authorizatio	08-Feb-22	3.5	Grafana is an open-source platform for monitoring and	https://github.com/grafa	A-GRA-GRAF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			observability. Affected versions of Grafana expose multiple API endpoints which do not properly handle user authorization. `/teams/:teamId` will allow an authenticated attacker to view unintended data by querying for the specific team ID, `/teams/:search` will allow an authenticated attacker to search for teams and see the total number of available teams, including for those teams that the user does not have access to, and `/teams/:teamId/members` when editors_can_admin flag is enabled, an authenticated attacker can see unintended data by querying for the specific team ID. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-21713**	na/grafana/pull/45083, https://grafana.com/blog/2022/02/08/grafana-7.5.15-and-8.3.5-released-with-moderate-severity-security-fixes/, https://github.com/grafana/grafana/security/advisories/GHSA-63g3-9jq3-mccv	170222/110
hyphp					
hybbs2					
Unrestricted Upload of File with Dangerous Type	09-Feb-22	6.5	update_code in Admin.php in HYBBS2 through 2.3.2 allows arbitrary file upload via a crafted ZIP archive. **CVE ID : CVE-2022-24676**	N/A	A-HYP-HYBB-170222/111
N/A	09-Feb-22	7.5	Admin.php in HYBBS2 through 2.3.2 allows remote code execution because it writes plugin-related configuration information to conf.php.	N/A	A-HYP-HYBB-170222/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24677		
Insyde					
insydeh2o					
Out-of-bounds Write	03-Feb-22	10	An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM. **CVE ID : CVE-2022-24030**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022011	A-INS-INSY-170222/113
Out-of-bounds Write	03-Feb-22	7.2	An issue was discovered in NvmExpressDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM. **CVE ID : CVE-2022-24031**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022015	A-INS-INSY-170222/114
N/A	03-Feb-22	7.2	An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.0 before 05.08.41, 5.1 before 05.16.29, 5.2 before 05.26.29, 5.3 before 05.35.29, 5.4 before 05.43.29, and 5.5 before 05.51.29. An SMM callout vulnerability allows an attacker to hijack the execution flow of code running in System Management Mode. Exploiting this issue could	https://www.insyde.com/security-pledge	A-INS-INSY-170222/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to escalating privileges to SMM. **CVE ID : CVE-2022-24069**		
Intel					
quartus_prime					
Improper Preservation of Permissions	09-Feb-22	4.6	Improper permissions in the SafeNet Sentinel driver for Intel(R) Quartus(R) Prime Standard Edition before version 21.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-21203**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00632.html	A-INT-QUAR-170222/116
Incorrect Default Permissions	09-Feb-22	4.6	Improper permissions for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-21204**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00632.html	A-INT-QUAR-170222/117
Improper Restriction of XML External Entity Reference	09-Feb-22	5	Improper restriction of XML external entity reference in DSP Builder Pro for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2022-21205**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00632.html	A-INT-QUAR-170222/118
Improper Restriction of XML External Entity Reference	09-Feb-22	4.6	Improper restriction of XML external entity for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable	https://www.intel.com/content/www/us/en/security-center/advis	A-INT-QUAR-170222/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege via local access. **CVE ID : CVE-2022-21220**	ory/intel-sa-00632.html	
trace_analyzer_and_collector					
Out-of-bounds Read	09-Feb-22	2.1	Out-of-bounds read in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2022-21133**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00639.html	A-INT-TRAC-170222/120
Access of Uninitialized Pointer	09-Feb-22	2.1	Access of uninitialized pointer in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2022-21156**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00639.html	A-INT-TRAC-170222/121
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	Uncaught exception in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2022-21218**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00639.html	A-INT-TRAC-170222/122
Out-of-bounds Read	09-Feb-22	2.1	Out-of-bounds read in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2022-21226**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00639.html	A-INT-TRAC-170222/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
itextpdf					
itext					
Allocation of Resources Without Limits or Throttling	01-Feb-22	4.3	iText v7.1.17 was discovered to contain an out-of-memory error via the component readStreamBytesRaw, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file. **CVE ID : CVE-2022-24196**	N/A	A-ITE-ITEX-170222/124
Out-of-bounds Write	01-Feb-22	4.3	iText v7.1.17 was discovered to contain a stack-based buffer overflow via the component ByteBuffer.append, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file. **CVE ID : CVE-2022-24197**	N/A	A-ITE-ITEX-170222/125
Out-of-bounds Read	01-Feb-22	4.3	iText v7.1.17 was discovered to contain an out-of-bounds exception via the component ARCFOUREncryption.encrypt ARCFOUR, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file. **CVE ID : CVE-2022-24198**	N/A	A-ITE-ITEX-170222/126
itunesrpc-remastered_project					
itunesrpc-remastered					
Improper Neutralization of Input During Web Page Generation ('Cross-site	01-Feb-22	4.3	iTunesRPC-Remastered is a discord rich presence application for use with iTunes & Apple Music. In code before commit 24f43aa user input is not properly sanitized and code injection is possible. Users are advised	https://github.com/bildsben/iTunesRPC-Remastered/security/advisories/GHSA-3xpp-rhqx-	A-ITU-ITUN-170222/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			to upgrade as soon as is possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-23603**	cw96, https://github.com/bildsben/iTunesRPC-Remastered/commit/54b02d9f3a94de94e4fb471908b8cf798e62e411	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Feb-22	6.4	iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible. **CVE ID : CVE-2022-23609**	https://github.com/bildsben/iTunesRPC-Remastered/security/advisories/GHSA-cc8j-fr7v-7r6q, https://github.com/bildsben/iTunesRPC-Remastered/commit/1eb1e5428f0926b2829a0bbbb65b0d946e608593	A-ITU-ITUN-170222/128
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-22	7.5	iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize image file paths leading to OS level command injection. This issue has been patched in commit cdcd48b. Users are advised to upgrade.	https://github.com/bildsben/iTunesRPC-Remastered/security/advisories/GHSA-mjv7-r62p-vhhg, https://githu	A-ITU-ITUN-170222/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23611	b.com/bildsben/iTunesRPC-Remastered/commit/cdcd48bbc44009ddcbd07a809b87376dc9ce37f4	
Jenkins					
jenkins					
Deserialization of Untrusted Data	09-Feb-22	5	Jenkins 2.333 and earlier, LTS 2.319.2 and earlier defines custom XStream converters that have not been updated to apply the protections for the vulnerability CVE-2021-43859 and allow unconstrained resource usage. **CVE ID : CVE-2022-0538**	https://www.jenkins.io/security/advisory/2022-02-09/#SECURITY-2602	A-JEN-JENK-170222/130
joinmastodon					
mastodon					
Incorrect Authorization	03-Feb-22	7.5	Mastodon before 3.3.2 and 3.4.x before 3.4.6 has incorrect access control because it does not compact incoming signed JSON-LD activities. (JSON-LD signing has been supported since version 1.6.0.) **CVE ID : CVE-2022-24307**	https://github.com/mastodon/mastodon/releases/tag/v3.3.2, https://github.com/mastodon/mastodon/releases/tag/v3.4.6	A-JOI-MAST-170222/131
Improperly Controlled Modification of Object Prototype	02-Feb-22	4.3	Prototype Pollution in GitHub repository mastodon/mastodon prior to 3.5.0. **CVE ID : CVE-2022-0432**	https://huntr.dev/bounties/d06da292-7716-4d74-a129-	A-JOI-MAST-170222/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Attributes ('Prototype Pollution')				dd04773398d7, https://github.com/mastodon/mastodon/commit/4d6d4b43c6186a13e67b92eaf70fe1b70ea24a09	
joplin_project					
joplin					
N/A	08-Feb-22	7.5	Joplin 2.6.10 allows remote attackers to execute system commands through malicious code in user search results. **CVE ID : CVE-2022-23340**	N/A	A-JOP-JOPL-170222/133
jpress					
jpress					
N/A	04-Feb-22	6.5	A remote code execution (RCE) vulnerability in HelloWorldAddonController.java of jpress v4.2.0 allows attackers to execute arbitrary code via a crafted JAR package. **CVE ID : CVE-2022-23330**	N/A	A-JPR-JPRE-170222/134
junrar_project					
junrar					
Loop with Unreachable Exit Condition ('Infinite Loop')	01-Feb-22	5	Junrar is an open source java RAR archive library. In affected versions A carefully crafted RAR archive can trigger an infinite loop while extracting said archive. The impact depends solely on how the application uses the	https://github.com/junrar/junrar/security/advisories/GHSA-m6cj-93v6-cvr5, https://githu	A-JUN-JUNR-170222/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			library, and whether files can be provided by malignant users. The problem is patched in 7.4.1. There are no known workarounds and users are advised to upgrade as soon as possible. **CVE ID : CVE-2022-23596**	b.com/junrar/junrar/commit/7b16b3d90b91445fd6af0adfed22c07413d4fab7	
karma_project					
karma					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Feb-22	4.3	Cross-site Scripting (XSS) - DOM in NPM karma prior to 6.3.14. **CVE ID : CVE-2022-0437**	https://huntr.dev/bounties/64b67ea1-5487-4382-a5f6-e8a95f798885, https://github.com/karma-runner/karma/commit/839578c45a8ac42fbc1d72105f97eab77dd3eb8a	A-KAR-KARM-170222/136
keybase					
keybase					
Exposure of Sensitive Information to an Unauthorized Actor	09-Feb-22	4.3	The Keybase Clients for macOS and Windows before version 5.9.0 fails to properly remove exploded messages initiated by a user. This can occur if the receiving user switches to a non-chat feature and places the host in a sleep state before the sending user explodes the messages. This could lead to	https://explore.zoom.us/en/trust/security/security-bulletin	A-KEY-KEYB-170222/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure of sensitive information which was meant to be deleted from a user's filesystem. **CVE ID : CVE-2022-22779**		
kicad					
kicad_eda					
Out-of-bounds Write	04-Feb-22	6.8	A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon GCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-23946**	N/A	A-KIC-KICA-170222/138
Out-of-bounds Write	04-Feb-22	6.8	A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon DCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-23947**	N/A	A-KIC-KICA-170222/139
laracom_project					
laracom					
Improper Neutralization of Input	04-Feb-22	3.5	Unrestricted Upload of File with Dangerous Type in Packagist jsdecena/laracom	https://huntr.dev/bounties/cb5b8563	A-LAR-LARA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			prior to v2.0.9. **CVE ID : CVE-2022-0472**	-15cf-408c-9f79-4871ea0a8713, https://github.com/jsdecena/laracom/commit/256026193ce994dc4c1365e02f414d8a0cd77ae8	170222/140
Linuxfoundation					
argo-cd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Feb-22	4	Argo CD before 2.1.9 and 2.2.x before 2.2.4 allows directory traversal related to Helm charts because of an error in helmTemplate in repository.go. For example, an attacker may be able to discover credentials stored in a YAML file. **CVE ID : CVE-2022-24348**	https://github.com/argoproj/argo-cd/security/advisories/GHSA-63qx-x74g-jcr7	A-LIN-ARGO-170222/141
livehelperchat					
live_helper_chat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v. **CVE ID : CVE-2022-0502**	https://github.com/livehelperchat/livehelperchat/commit/d3b107aaa8ec10816acc762d60e7321079c21706, https://hunter.dev/bounties/34f2aa30-de7f-432a-	A-LIV-LIVE-170222/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				8749-b43d2774140f	
Mahara					
mahara					
Files or Directories Accessible to External Parties	09-Feb-22	4	In Mahara 20.10 before 20.10.4, 21.04 before 21.04.3, and 21.10 before 21.10.1, the names of folders in the Files area can be seen by a person not owning the folders. (Only folder names are affected. Neither file names nor file contents are affected.) **CVE ID : CVE-2022-24694**	https://mahara.org/interaction/forum/topic.php?id=8994	A-MAH-MAHA-170222/143
Microsoft					
.net					
N/A	09-Feb-22	4.3	.NET Denial of Service Vulnerability. **CVE ID : CVE-2022-21986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21986	A-MIC-.NET-170222/144
365_apps					
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Office Information Disclosure Vulnerability. **CVE ID : CVE-2022-23252**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23252	A-MIC-365_-170222/145
N/A	09-Feb-22	6.8	Microsoft Office Visio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-365_-170222/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2022-21988	
N/A	09-Feb-22	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22003	A-MIC-365_-170222/147
N/A	09-Feb-22	6.8	Microsoft Office ClickToRun Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22004**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22004	A-MIC-365_-170222/148
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-365_-170222/149
azure_data_explorer					
N/A	09-Feb-22	4.3	Azure Data Explorer Spoofing Vulnerability. **CVE ID : CVE-2022-23256**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23256	A-MIC-AZUR-170222/150
dynamics_365					
N/A	09-Feb-22	6.5	Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21957**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21957	A-MIC-DYNA-170222/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dynamics_gp					
N/A	09-Feb-22	4.3	Microsoft Dynamics GP Spoofing Vulnerability. **CVE ID : CVE-2022-23269**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23269	A-MIC-DYNA-170222/152
Improper Privilege Management	09-Feb-22	9	Microsoft Dynamics GP Elevation Of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23272, CVE-2022-23273. **CVE ID : CVE-2022-23271**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23271	A-MIC-DYNA-170222/153
Improper Privilege Management	09-Feb-22	9	Microsoft Dynamics GP Elevation Of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23271, CVE-2022-23273. **CVE ID : CVE-2022-23272**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23272	A-MIC-DYNA-170222/154
Improper Privilege Management	09-Feb-22	9	Microsoft Dynamics GP Elevation Of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23271, CVE-2022-23272. **CVE ID : CVE-2022-23273**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23273	A-MIC-DYNA-170222/155
N/A	09-Feb-22	6.5	Microsoft Dynamics GP Remote Code Execution Vulnerability. **CVE ID : CVE-2022-23274**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23274	A-MIC-DYNA-170222/156
edge_chromium					
N/A	07-Feb-22	5	Microsoft Edge (Chromium-based) Tampering	https://portal.msrc.micr	A-MIC-EDGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. **CVE ID : CVE-2022-23261**	osoft.com/en-US/security-guidance/advisory/CVE-2022-23261	170222/157
Improper Privilege Management	07-Feb-22	6.8	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23263. **CVE ID : CVE-2022-23262**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23262	A-MIC-EDGE-170222/158
Improper Privilege Management	07-Feb-22	4.4	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23262. **CVE ID : CVE-2022-23263**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23263	A-MIC-EDGE-170222/159
excel					
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-EXCE-170222/160
office					
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Office Information Disclosure Vulnerability. **CVE ID : CVE-2022-23252**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23252	A-MIC-OFFI-170222/161
N/A	09-Feb-22	6.8	Microsoft Office Visio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21988**	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-OFFI-170222/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2022-21988	
N/A	09-Feb-22	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22003	A-MIC-OFFI-170222/163
N/A	09-Feb-22	6.8	Microsoft Office ClickToRun Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22004**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22004	A-MIC-OFFI-170222/164
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-OFFI-170222/165
office_long_term_servicing_channel					
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Office Information Disclosure Vulnerability. **CVE ID : CVE-2022-23252**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23252	A-MIC-OFFI-170222/166
N/A	09-Feb-22	6.8	Microsoft Office Visio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21988	A-MIC-OFFI-170222/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Feb-22	6.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22003	A-MIC-OFFI-170222/168
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-OFFI-170222/169
office_online_server					
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-OFFI-170222/170
office_web_apps					
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-OFFI-170222/171
onedrive					
Incorrect Authorization	09-Feb-22	4.6	Microsoft OneDrive for Android Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-23255**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23255	A-MIC-ONED-170222/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
outlook_2016					
N/A	09-Feb-22	5	Microsoft Outlook for Mac Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-23280**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23280	A-MIC-OUTL-170222/173
powerbi-client_js_sdk					
Exposure of Resource to Wrong Sphere	09-Feb-22	4	Microsoft Power BI Information Disclosure Vulnerability. **CVE ID : CVE-2022-23254**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23254	A-MIC-POWE-170222/174
sharepoint_enterprise_server					
Improper Authentication	09-Feb-22	4	Microsoft SharePoint Server Security Feature BypassVulnerability. **CVE ID : CVE-2022-21968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21968	A-MIC-SHAR-170222/175
N/A	09-Feb-22	6	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-21987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21987	A-MIC-SHAR-170222/176
N/A	09-Feb-22	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22005**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22005	A-MIC-SHAR-170222/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sharepoint_foundation					
Improper Authentication	09-Feb-22	4	Microsoft SharePoint Server Security Feature BypassVulnerability. **CVE ID : CVE-2022-21968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21968	A-MIC-SHAR-170222/178
N/A	09-Feb-22	6	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-21987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21987	A-MIC-SHAR-170222/179
N/A	09-Feb-22	6.5	Microsoft SharePoint Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22005**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22005	A-MIC-SHAR-170222/180
sharepoint_server					
Improper Authentication	09-Feb-22	4	Microsoft SharePoint Server Security Feature BypassVulnerability. **CVE ID : CVE-2022-21968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21968	A-MIC-SHAR-170222/181
N/A	09-Feb-22	6	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-21987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21987	A-MIC-SHAR-170222/182
N/A	09-Feb-22	6.5	Microsoft SharePoint Server Remote Code Execution	https://portal.msrc.micr	A-MIC-SHAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. **CVE ID : CVE-2022-22005**	osoft.com/en-US/security-guidance/advisory/CVE-2022-22005	170222/183
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-22716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22716	A-MIC-SHAR-170222/184
sql_server					
Improper Privilege Management	09-Feb-22	4.6	SQL Server for Linux Containers Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23276	A-MIC-SQL_-170222/185
teams					
N/A	09-Feb-22	5	Microsoft Teams Denial of Service Vulnerability. **CVE ID : CVE-2022-21965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21965	A-MIC-TEAM-170222/186
visual_studio_2019					
N/A	09-Feb-22	4.3	.NET Denial of Service Vulnerability. **CVE ID : CVE-2022-21986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21986	A-MIC-VISU-170222/187
visual_studio_2022					
N/A	09-Feb-22	4.3	.NET Denial of Service	https://port	A-MIC-VISU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. **CVE ID : CVE-2022-21986**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21986	170222/188
visual_studio_code					
N/A	09-Feb-22	7.5	Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21991	A-MIC-VISU-170222/189
vp9_video_extensions					
N/A	09-Feb-22	6.8	VP9 Video Extensions Remote Code Execution Vulnerability. **CVE ID : CVE-2022-22709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22709	A-MIC-VP9_-170222/190
Microweber					
microweber					
Generation of Error Message Containing Sensitive Information	08-Feb-22	4	Generation of Error Message Containing Sensitive Information in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0504**	https://github.com/microweber/microweber/commit/e607e5f745cd99d5c06a7fce16b3577fab8e1250, https://huntr.dev/bounties/285ff8a0-a273-4d62-ba01-3e4b4e1846	A-MIC-MICR-170222/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				7b	
Cross-Site Request Forgery (CSRF)	08-Feb-22	4.3	Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0505**	https://github.com/microweber/microweber/commit/63447b369973724f0d352a006f25af6ff71ae292, https://huntr.dev/bounties/65b5a243-3f0c-4df3-9bab-898332180968	A-MIC-MICR-170222/192
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0506**	https://huntr.dev/bounties/0a5ec24c-343e-4cc4-b27b-2beb19a1c35f, https://github.com/microweber/microweber/commit/05d55f2befb1b25375ca5371875ff535d6cc5f70	A-MIC-MICR-170222/193
minetest					
minetest					
Improper Neutralization of Special Elements in Output Used	02-Feb-22	7.5	Minetest before 5.4.0 allows attackers to add or modify arbitrary meta fields of the same item stack as saved user input, aka ItemStack meta	https://github.com/minetest/minetest/security/advisories/GHS	A-MIN-MINE-170222/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			injection. **CVE ID : CVE-2022-24300**	A-hwj2-xf72-r4cf, https://github.com/minetest/minetest/commit/b5956bde259faa240a81060ff4e598e25ad52dae, https://bugs.debian.org/1004223	
Incorrect Default Permissions	02-Feb-22	6.4	In Minetest before 5.4.0, players can add or subtract items from a different player's inventory. **CVE ID : CVE-2022-24301**	https://github.com/minetest/minetest/commit/3693b6871eba268ecc79b3f52d00d3cefe761131	A-MIN-MINE-170222/195
mirantis					
container_cloud_lens_extension					
Improper Input Validation	04-Feb-22	6.8	Lack of validation of URLs causes Mirantis Container Cloud Lens Extension before v3.1.1 to open external programs other than the default browser to perform sign on to a new cluster. An attacker could host a webserver which serves a malicious Mirantis Container Cloud configuration file and induce the victim to add a new cluster via its URL. This issue affects: Mirantis Mirantis Container Cloud Lens Extension v3 versions	N/A	A-MIR-CONT-170222/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to v3.1.1. **CVE ID : CVE-2022-0484**		
Mozilo					
mozilo					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Feb-22	6.4	mozilo2.0 was discovered to be vulnerable to directory traversal attacks via the parameter curent_dir. **CVE ID : CVE-2022-23357**	N/A	A-MOZ-MOZI-170222/197
mruby					
mruby					
NULL Pointer Dereference	04-Feb-22	7.8	NULL Pointer Dereference in Homebrew mruby prior to 3.2. **CVE ID : CVE-2022-0481**	https://huntr.dev/bounties/54725c8c-87f4-41b6-878c-01d8e0ee7027, https://github.com/mruby/mruby/commit/ae3c99767a27f5c6c584162e2adc6a5d0eb2c54e	A-MRU-MRUB-170222/198
Out-of-bounds Read	09-Feb-22	6.4	Out-of-bounds Read in Homebrew mruby prior to 3.2. **CVE ID : CVE-2022-0525**	https://huntr.dev/bounties/e19e109f-acf0-4048-8ee8-1b10a870f1e9, https://github.com/mrub	A-MRU-MRUB-170222/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				y/mruby/commit/0849a2885f81cfd82134992c06df3ccd59052ac7	
nats					
nats_server					
Incorrect Authorization	08-Feb-22	9	NATS nats-server before 2.7.2 has Incorrect Access Control. Any authenticated user can obtain the privileges of the System account by misusing the "dynamically provisioned sandbox accounts" feature. **CVE ID : CVE-2022-24450**	https://advisories.nats.io/CVE/CVE-2022-24450.txt	A-NAT-NATS-170222/200
nats_streaming_server					
Incorrect Authorization	08-Feb-22	9	NATS nats-server before 2.7.2 has Incorrect Access Control. Any authenticated user can obtain the privileges of the System account by misusing the "dynamically provisioned sandbox accounts" feature. **CVE ID : CVE-2022-24450**	https://advisories.nats.io/CVE/CVE-2022-24450.txt	A-NAT-NATS-170222/201
neutrinolabs					
xrdp					
Integer Underflow (Wrap or Wraparound)	07-Feb-22	7.2	xrdp is an open source remote desktop protocol (RDP) server. In affected versions an integer underflow leading to a heap overflow in the sesman server allows any unauthenticated attacker which is able to locally access a sesman server to execute code as root. This	https://github.com/neutrinolabs/xrdp/commit/4def30ab8ea445cdc06832a44c3ec40a506a0ffa, https://github.com/neutrinolabs/xrdp	A-NEU-XRDP-170222/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been patched in version 0.9.18.1 and above. Users are advised to upgrade. There are no known workarounds. **CVE ID : CVE-2022-23613**	/security/advisories/GHSA-8h98-h426-xf32	
nim-lang					
docutils					
Improper Authentication	01-Feb-22	5.5	Nimforum is a lightweight alternative to Discourse written in Nim. In versions prior to 2.2.0 any forum user can create a new thread/post with an include referencing a file local to the host operating system. Nimforum will render the file if able. This can also be done silently by using NimForum's post "preview" endpoint. Even if NimForum is running as a non-critical user, the forum.json secrets can be stolen. Version 2.2.0 of NimForum includes patches for this vulnerability. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-23602**	https://github.com/nim-lang/nimforum/security/advisories/GHSA-q3vh-x957-wr75, https://github.com/nim-lang/Nim/commit/cb894c7094fb49014f85815a9dafc38b5dda743e	A-NIM-DOCU-170222/203
nimforum					
Improper Authentication	01-Feb-22	5.5	Nimforum is a lightweight alternative to Discourse written in Nim. In versions prior to 2.2.0 any forum user can create a new thread/post with an include referencing a file local to the host operating	https://github.com/nim-lang/nimforum/security/advisories/GHSA-q3vh-x957-wr75,	A-NIM-NIMF-170222/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. Nimforum will render the file if able. This can also be done silently by using NimForum's post "preview" endpoint. Even if NimForum is running as a non-critical user, the forum.json secrets can be stolen. Version 2.2.0 of NimForum includes patches for this vulnerability. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-23602**	https://github.com/nim-lang/Nim/commit/cb894c7094fb49014f85815a9dafc38b5dda743e	
Nvidia					
gpu_display_driver					
Improper Handling of Exceptional Conditions	07-Feb-22	3.6	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel driver, where improper handling of insufficient permissions or privileges may allow an unprivileged local user limited write access to protected memory, which can lead to denial of service. **CVE ID : CVE-2022-21813**	https://nvidia.custhelp.com/app/answers/detail/a_id/5321	A-NVI-GPU_-170222/205
Improper Handling of Exceptional Conditions	07-Feb-22	3.6	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel driver package, where improper handling of insufficient permissions or privileges may allow an unprivileged local user limited write access to	https://nvidia.custhelp.com/app/answers/detail/a_id/5321	A-NVI-GPU_-170222/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protected memory, which can lead to denial of service. **CVE ID : CVE-2022-21814**		
NULL Pointer Dereference	07-Feb-22	4.9	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for private IOCTLs where a NULL pointer dereference in the kernel, created within user mode code, may lead to a denial of service in the form of a system crash. **CVE ID : CVE-2022-21815**	https://nvidia.custhelp.com/app/answers/detail/a_id/5321	A-NVI-GPU_-170222/207
omniverse_launcher					
Exposure of Resource to Wrong Sphere	02-Feb-22	5.8	NVIDIA Omniverse Launcher contains a Cross-Origin Resource Sharing (CORS) vulnerability which can allow an unprivileged remote attacker, if they can get user to browse malicious site, to acquire access tokens allowing them to access resources in other security domains, which may lead to code execution, escalation of privileges, and impact to confidentiality and integrity. **CVE ID : CVE-2022-21817**	https://nvidia.custhelp.com/app/answers/detail/a_id/5318	A-NVI-OMNI-170222/208
virtual_gpu					
N/A	07-Feb-22	4.9	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (nvidia.ko), where a user in the guest OS can cause a GPU interrupt storm on the	https://nvidia.custhelp.com/app/answers/detail/a_id/5321, https://nvidi	A-NVI-VIRT-170222/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hypervisor host, leading to a denial of service. **CVE ID : CVE-2022-21816**	a.custhelp.com/app/answers/detail/a_id/5312	
octopus					
octopus_deploy					
URL Redirection to Untrusted Site ('Open Redirect')	07-Feb-22	5.8	In affected Octopus Server versions when the server HTTP and HTTPS bindings are configured to localhost, Octopus Server will allow open redirects. **CVE ID : CVE-2022-23184**	https://advisories.octopus.com/post/2022/sa2022-02/	A-OCT-OCTO-170222/210
Otrs					
otrs					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-22	3.5	OTRS administrators can configure dynamic field and inject malicious JavaScript code in the error message of the regular expression check. When used in the agent interface, malicious code might be exectued in the browser. This issue affects: OTRS AG OTRS 7.0.x version: 7.0.31 and prior versions. **CVE ID : CVE-2022-0473**	https://otrs.com/release-notes/otrs-security-advisory-2022-01/	A-OTR-OTRS-170222/211
Exposure of Sensitive Information to an Unauthorized Actor	07-Feb-22	3.5	Full list of recipients from customer users in a contact field could be disclosed in notification emails event when the notification is set to be sent to each recipient individually. This issue affects: OTRS AG OTRSCustomContactFields 8.0.x version: 8.0.11 and prior versions.	https://otrs.com/release-notes/otrs-security-advisory-2022-02/	A-OTR-OTRS-170222/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0474		
Pimcore					
pimcore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.3.1. **CVE ID : CVE-2022-0509**	https://huntr.dev/bounties/26cdf86c-8edc-4af6-8411-d569699ecd1b, https://github.com/pimcore/pimcore/commit/6ccb5c12fc1be065ebce9c89c4677ee939b88597	A-PIM-PIMC-170222/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	3.5	Cross-site Scripting (XSS) - Reflected in Packagist pimcore/pimcore prior to 10.3.1. **CVE ID : CVE-2022-0510**	https://github.com/pimcore/pimcore/commit/b5a9ad65e5a4dde1916f02019f8686ad835681ce, https://huntr.dev/bounties/bb3525d5-dedc-48b8-ab04-ad4c72499abe	A-PIM-PIMC-170222/214
Postgresql					
pgjdbc					
Exposure of Resource to Wrong	02-Feb-22	7.5	pgjdbc is the offical PostgreSQL JDBC Driver. A security hole was found in the jdbc driver for postgresql	https://github.com/pgjdbc/pgjdbc/security/adviso	A-POS-PGJD-170222/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnameverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-21724**	ries/GHSA-v7wg-cpwc-24m4, https://github.com/pgjdbc/pgjdbc/commit/f4d0ed69c0b3aae8531d83d6af4c57f22312c813	
premio					
mystickyelements					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-22	3.5	The All-in-one Floating Contact Form, Call, Chat, and 50+ Social Icon Tabs WordPress plugin before 2.0.4 was vulnerable to reflected XSS on the my-sticky-elements-leads admin page. **CVE ID : CVE-2022-0148**	https://plugins.trac.wordpress.org/changeset/2654453/mystickyelements	A-PRE-MYST-170222/216
publify_project					
publify					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Feb-22	5	Business Logic Errors in GitHub repository publify/publify prior to 9.2.7. **CVE ID : CVE-2022-0524**	https://github.com/publify/publify/commit/16fceecadbe80ab0ef846b62a12dc7bfff10b8c5, https://huntr.dev/bounties/bfffae58-b3cd-4e0e-b1f2-3db387a22c3d	A-PUB-PUBL-170222/217
Radare					
radare2					
NULL Pointer Dereference	01-Feb-22	4.3	NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.0. **CVE ID : CVE-2022-0419**	https://huntr.dev/bounties/1f84e79d-70e7-4b29-8b48-a108f81c89aa, https://github.com/radareorg/radare2/commit/feaa4e7f7399c51ee6f52deb84dc3f795b4035d6	A-RAD-RADA-170222/218
Heap-based Buffer Overflow	08-Feb-22	5.8	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.2. **CVE ID : CVE-2022-0518**	https://github.com/radareorg/radare2/commit/9650e3c352f675687bf6c6f65ff2c4a3d0e288fa,	A-RAD-RADA-170222/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://hunter.dev/bounties/10051adf-7ddc-4042-8fd0-8e9e0c5b1184	
Buffer Access with Incorrect Length Value	08-Feb-22	5.8	Buffer Access with Incorrect Length Value in GitHub repository radareorg/radare2 prior to 5.6.2. **CVE ID : CVE-2022-0519**	https://github.com/radareorg/radare2/commit/6c4428f018d385fc80a33ecddcb37beceа685dd5, https://hunter.dev/bounties/af85b9e1-d1cf-4c0e-ba12-525b82b7c1e3	A-RAD-RADA-170222/220
Use After Free	08-Feb-22	6.8	Use After Free in NPM radare2.js prior to 5.6.2. **CVE ID : CVE-2022-0520**	https://github.com/radareorg/radare2/commit/8525ad0b9fd596f4b251bb3d7b114e6dc7ce1ee8, https://hunter.dev/bounties/ce13c371-e5ef-4993-97f3-3d33dcd943a6	A-RAD-RADA-170222/221
Access of Memory Location	08-Feb-22	5.8	Access of Memory Location After End of Buffer in GitHub repository	https://github.com/radareorg/radare	A-RAD-RADA-170222/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
After End of Buffer			radareorg/radare2 prior to 5.6.2. **CVE ID : CVE-2022-0521**	2/commit/6c4428f018d385fc80a33ecddcb37beceа685dd5, https://huntr.dev/bounties/4d436311-bbf1-45a3-8774-bdb666d7f7ca	
Access of Memory Location Before Start of Buffer	08-Feb-22	5.8	Access of Memory Location Before Start of Buffer in NPM radare2.js prior to 5.6.2. **CVE ID : CVE-2022-0522**	https://huntr.dev/bounties/2d45e589-d614-4875-bba1-be0f729e7ca9, https://github.com/radareorg/radare2/commit/d17a7bdf166108a29a27cd89bf454f9fa6c050d6	A-RAD-RADA-170222/223
Expired Pointer Dereference	08-Feb-22	6.8	Expired Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.2. **CVE ID : CVE-2022-0523**	https://github.com/radareorg/radare2/commit/35482cb760db10f87a62569e2f8872dbd95e9269, https://huntr.dev/bounties/9d8d6ae0-fe00-40b9-ae1e-	A-RAD-RADA-170222/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b0e8103bac69	
Use After Free	08-Feb-22	7.5	Use After Free in GitHub repository radareorg/radare2 prior to 5.6.0. **CVE ID : CVE-2022-0139**	https://github.com/radareorg/radare2/commit/37897226a1a31f982bfefdc4aeefc2e50355c73c, https://huntr.dev/bounties/3dcb6f40-45cd-403b-929f-db123fde32c0	A-RAD-RADA-170222/225
SAP					
content_server					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Feb-22	10	SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are vulnerable for request smuggling and request concatenation. An unauthenticated attacker can prepend a victim's request with arbitrary data. This way, the attacker can execute functions impersonating the victim or poison intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system. **CVE ID : CVE-2022-22536**	https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022, https://launchpad.support.sap.com/#/notes/3123396	A-SAP-CONT-170222/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
netweaver_application_server_java					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Feb-22	7.5	In SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an unauthenticated attacker could submit a crafted HTTP server request which triggers improper shared memory buffer handling. This could allow the malicious payload to be executed and hence execute functions that could be impersonating the victim or even steal the victim's logon session. **CVE ID : CVE-2022-22532**	https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022, https://launchpad.support.sap.com/#/notes/3123427	A-SAP-NETW-170222/227
Use After Free	09-Feb-22	5	Due to improper error handling in SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an attacker could submit multiple HTTP server requests resulting in errors, such that it consumes the memory buffer. This could result in system shutdown rendering the system unavailable. **CVE ID : CVE-2022-22533**	https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022, https://launchpad.support.sap.com/#/notes/3123427	A-SAP-NETW-170222/228
netweaver_as_abap					
Inconsistent Interpretation of HTTP	09-Feb-22	10	SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java,	https://wiki.scn.sap.com/wiki/display	A-SAP-NETW-170222/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Requests ('HTTP Request Smuggling')			ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are vulnerable for request smuggling and request concatenation. An unauthenticated attacker can prepend a victim's request with arbitrary data. This way, the attacker can execute functions impersonating the victim or poison intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system. **CVE ID : CVE-2022-22536**	/PSR/SAP+Security+Patch+Day+-+February+2022, https://launchpad.support.sap.com/#/notes/3123396	
web_dispatcher					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Feb-22	10	SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are vulnerable for request smuggling and request concatenation. An unauthenticated attacker can prepend a victim's request with arbitrary data. This way, the attacker can execute functions impersonating the victim or poison intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system. **CVE ID : CVE-2022-22536**	https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022, https://launchpad.support.sap.com/#/notes/3123396	A-SAP-WEB_-170222/230
Schneider-electric					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ecostruxure_power_monitoring_expert					
Improper Input Validation	04-Feb-22	4	A CWE-20: Improper Input Validation vulnerability exists that could allow arbitrary files on the server to be read by authenticated users through a limited operating system service account. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior) **CVE ID : CVE-2022-22726**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-07	A-SCH-ECOS-170222/231
Improper Input Validation	04-Feb-22	9.3	A CWE-20: Improper Input Validation vulnerability exists that could allow an unauthenticated attacker to view data, change settings, impact availability of the software, or potentially impact a user?s local machine when the user clicks a specially crafted link. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior) **CVE ID : CVE-2022-22727**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-07	A-SCH-ECOS-170222/232
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-22	3.5	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an authenticated attacker to view data, change settings, or impact availability of the software when the user visits a page containing the injected payload. Affected Product:	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-07	A-SCH-ECOS-170222/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Power Monitoring Expert (Versions 2020 and prior) **CVE ID : CVE-2022-22804**		
interactive_graphical_scada_system_data_server					
Out-of-bounds Read	09-Feb-22	5	A CWE-125: Out-of-bounds Read vulnerability exists that could cause memory leaks potentially resulting in denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior) **CVE ID : CVE-2022-24314**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-039-01	A-SCH-INTE-170222/234
Out-of-bounds Read	09-Feb-22	5	A CWE-125: Out-of-bounds Read vulnerability exists that could cause denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior) **CVE ID : CVE-2022-24315**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-039-01, https://www.zerodayinitiative.com/advisories/ZDI-22-322/	A-SCH-INTE-170222/235
Improper Initialization	09-Feb-22	5	A CWE-665: Improper Initialization vulnerability exists that could cause information exposure when an attacker sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-039-01, https://ww	A-SCH-INTE-170222/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior) **CVE ID : CVE-2022-24316**	w.zerodayinitiative.com/advisories/ZDI-22-323/	
Sensiolabs					
symfony					
Cross-Site Request Forgery (CSRF)	01-Feb-22	6.8	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony form component provides a CSRF protection mechanism by using a random token injected in the form and using the session to store and control the token submitted by the user. When using the FrameworkBundle, this protection can be enabled or disabled with the configuration. If the configuration is not specified, by default, the mechanism is enabled as long as the session is enabled. In a recent change in the way the configuration is loaded, the default behavior has been dropped and, as a result, the CSRF protection is not enabled in form when not explicitly enabled, which makes the application sensible to CSRF attacks. This issue has been resolved in the patch versions listed and users are advised to update. There are no known workarounds for this issue.	https://github.com/symfony/symfony/security/advisories/GHSA-vvmr-8829-6whx, https://github.com/symfony/symfony/commit/f0ffb775febdf07e57117aabadac96fa37857f50	A-SEN-SYMF-170222/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23601		
servisnet					
tessa					
Improper Authenticati on	06-Feb-22	7.5	An issue was discovered in Servisnet Tessa 0.0.2. An attacker can add a new sysadmin user via a manipulation of the Authorization HTTP header. **CVE ID : CVE-2022-22831**	N/A	A-SER-TESS-170222/238
Improper Privilege Management	06-Feb-22	10	An issue was discovered in Servisnet Tessa 0.0.2. Authorization data is available via an unauthenticated /data-service/users/ request. **CVE ID : CVE-2022-22832**	N/A	A-SER-TESS-170222/239
N/A	06-Feb-22	5	An issue was discovered in Servisnet Tessa 0.0.2. An attacker can obtain sensitive information via a /js/app.js request. **CVE ID : CVE-2022-22833**	http://www.servisnet.com.tr/en/page/products	A-SER-TESS-170222/240
Shibboleth					
oidc_op					
Server-Side Request Forgery (SSRF)	04-Feb-22	6.4	The OIDC OP plugin before 3.0.4 for Shibboleth Identity Provider allows server-side request forgery (SSRF) due to insufficient restriction of the request_uri parameter. This allows attackers to interact with arbitrary third-party HTTP services. **CVE ID : CVE-2022-24129**	http://shibboleth.net/community/advisories/, http://shibboleth.net/community/advisories/secadv_20220131.txt	A-SHI-OIDC-170222/241
Silverstripe					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
silverstripe					
N/A	04-Feb-22	4	Business Logic Errors in GitHub repository silverstripe/silverstripe-framework prior to 4.10.1. **CVE ID : CVE-2022-0227**	https://hunter.dev/bounties/35631e3a-f4b9-41ad-857c-7e3021932a72, https://github.com/silverstripe/silverstripe-framework/commit/cbf2987a616e9ef4d7eccae5d763ef2179bdbcc2	A-SIL-SILV-170222/242
starwindsoftware					
nas					
Improper Authentication	06-Feb-22	9	StarWind SAN and NAS before 0.2 build 1685 allows users to reset other users' passwords. **CVE ID : CVE-2022-24551**	N/A	A-STA-NAS-170222/243
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Feb-22	10	StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command. **CVE ID : CVE-2022-24552**	https://www.starwindsoftware.com/security/sw-20220203-0001/	A-STA-NAS-170222/244
san					
Improper Authentication	06-Feb-22	9	StarWind SAN and NAS before 0.2 build 1685 allows users to reset other users' passwords.	N/A	A-STA-SAN-170222/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24551		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Feb-22	10	StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command. **CVE ID : CVE-2022-24552**	https://www.starwindsoftware.com/security/sw-20220203-0001/	A-STA-SAN-170222/246
symfony					
twig					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Feb-22	7.5	Twig is an open source template language for PHP. When in a sandbox mode, the `arrow` parameter of the `sort` filter must be a closure to avoid attackers being able to run arbitrary PHP functions. In affected versions this constraint was not properly enforced and could lead to code injection of arbitrary PHP code. Patched versions now disallow calling non Closure in the `sort` filter as is the case for some other filters. Users are advised to upgrade. **CVE ID : CVE-2022-23614**	https://github.com/twigphp/Twig/commit/2eb330805586112 01b55079d0 7ac88f207b4 66d5, https://github.com/twigphp/Twig/commit/22b9d c3c03ee66d7 e21d9ed2ca 76052b134c b9e9, https://github.com/twigphp/Twig/security/advisories/GHSA-5mv2-rx3q-4w2v	A-SYM-TWIG-170222/247
Synology					
diskstation_manager					
Improper Limitation of a Pathname	07-Feb-22	4	Improper limitation of a pathname to a restricted directory ('Path Traversal')	https://www.synology.com/security	A-SYN-DISK-170222/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			vulnerability in support service management in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote authenticated users to write arbitrary files via unspecified vectors. **CVE ID : CVE-2022-22679**	/advisory/Synology_SA_22_01	
N/A	07-Feb-22	5	Exposure of sensitive information to an unauthorized actor vulnerability in Web Server in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote attackers to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2022-22680**	https://www.synology.com/security/advisory/Synology_SA_22_01	A-SYN-DISK-170222/249
taogogo					
taocms					
Files or Directories Accessible to External Parties	04-Feb-22	4	An issue was discovered in taoCMS v3.0.2. There is an arbitrary file read vulnerability that can read any files via admin.php?action=file&ctrl=download&path=../../1.txt. **CVE ID : CVE-2022-23316**	N/A	A-TAO-TAOC-170222/250
tastyigniter					
tastyigniter					
Improper Neutralization of Input During Web Page Generation	09-Feb-22	3.5	A Cross-Site Scripting (XSS) vulnerability exists within the 3.2.2 version of TastyIgniter. The "items%5B0%5D%5Bpath%5D" parameter of a request	N/A	A-TAS-TAST-170222/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			made to /admin/allergens/edit/1 is vulnerable. **CVE ID : CVE-2022-23378**		
Thedigitalcraft					
atomcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Feb-22	7.5	AtomCMS v2.0 was discovered to contain a SQL injection vulnerability via /admin/login.php. **CVE ID : CVE-2022-24223**	N/A	A-THE-ATOM-170222/252
Trendmicro					
worry-free_business_security					
Out-of-bounds Read	04-Feb-22	3.6	A security out-of-bounds read information disclosure vulnerability in Trend Micro Worry-Free Business Security Server could allow a local attacker to send garbage data to a specific named pipe and crash the server. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-23805**	https://success.trendmicro.com/solution/000290416	A-TRE-WORR-170222/253
twistedmatrix					
treq					
URL Redirection to Untrusted Site ('Open	01-Feb-22	4.3	treq is an HTTP library inspired by requests but written on top of Twisted's Agents. Treq's request	https://github.com/twisted/treq/security/advisorie	A-TWI-TREQ-170222/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			methods (`treq.get`, `treq.post`, etc.) and `treq.client.HTTPClient` constructor accept cookies as a dictionary. Such cookies are not bound to a single domain, and are therefore sent to *every* domain ("supercookies"). This can potentially cause sensitive information to leak upon an HTTP redirect to a different domain., e.g. should `https://example.com` redirect to `http://cloudstorageprovider.com` the latter will receive the cookie `session`. Treq 2021.1.0 and later bind cookies given to request methods (`treq.request`, `treq.get`, `HTTPClient.request`, `HTTPClient.get`, etc.) to the origin of the *url* parameter. Users are advised to upgrade. For users unable to upgrade Instead of passing a dictionary as the *cookies* argument, pass a `http.cookiejar.CookieJar` instance with properly domain- and scheme-scoped cookies in it. **CVE ID : CVE-2022-23607**	s/GHSA-fhpf-pp6p-55qc	
twisted					
Exposure of Sensitive Information to an	07-Feb-22	5	twisted is an event-driven networking engine written in Python. In affected versions twisted exposes cookies and	https://github.com/twisted/twisted/commit/af8fe7	A-TWI-TWIS-170222/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			authorization headers when following cross-origin redirects. This issue is present in the `twited.web.RedirectAgent` and `twisted.web.BrowserLikeRedirectAgent` functions. Users are advised to upgrade. There are no known workarounds. **CVE ID : CVE-2022-21712**	8542a6f2bf2235ccee8158d9c88d31e8e2, https://github.com/twisted/twisted/security/advisories/GHSA-92x2-jw7w-xvvx	
ujcms					
jspxcms					
Unrestricted Upload of File with Dangerous Type	04-Feb-22	7.5	A vulnerability in ${"freemarker.template.utility.Execute"?new() of UJCMS Jspxcms v10.2.0 allows attackers to execute arbitrary commands via uploading malicious files. **CVE ID : CVE-2022-23329**	N/A	A-UJC-JSPX-170222/256
unifiedoffice					
total_connect_now					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Feb-22	5	SQL Injection vulnerability discovered in Unified Office Total Connect Now that would allow an attacker to extract sensitive information through a cookie parameter. **CVE ID : CVE-2022-24121**	https://unifiedoffice.com/total-connect-now/	A-UNI-TOTA-170222/257
victor_cms_project					
victor_cms					
Improper Neutralization of Special	03-Feb-22	6.5	Victor CMS v1.0 was discovered to contain a SQL injection vulnerability that	N/A	A-VIC-VICT-170222/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			allows attackers to inject arbitrary commands via 'user_firstname' parameter. **CVE ID : CVE-2022-23873**		
VIM					
vim					
Heap-based Buffer Overflow	01-Feb-22	6.8	Heap-based Buffer Overflow GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-0417**	https://huntr.dev/bounties/fc86bc8d-c866-4ade-8b7f-e49cec306d1a, https://github.com/vim/vim/commit/652dee448618589de5528a9e9a36995803f5557a	A-VIM-VIM-170222/259
Use After Free	02-Feb-22	6.8	Use After Free in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-0443**	https://github.com/vim/vim/commit/9b4a80a66544f2782040b641498754bcb5b8d461, https://huntr.dev/bounties/b987c8cb-bbbe-4601-8a6c-54ff907c6b51	A-VIM-VIM-170222/260
visser					
store_exporter_for_woocommerce					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Feb-22	4.3	The WooCommerce Stored Exporter WordPress plugin before 2.7.1 was affected by a Reflected Cross-Site Scripting (XSS) vulnerability in the woo_ce admin page. **CVE ID : CVE-2022-0149**	https://plugins.trac.wordpress.org/changeset/2654545/woocommerce-exporter	A-VIS-STOR-170222/261
Vmware					
cloud_foundation					
Insertion of Sensitive Information into Log File	04-Feb-22	4	VMware Cloud Foundation contains an information disclosure vulnerability due to logging of credentials in plain-text within multiple log files on the SDDC Manager. A malicious actor with root access on VMware Cloud Foundation SDDC Manager may be able to view credentials in plaintext within one or more log files. **CVE ID : CVE-2022-22939**	https://www.vmware.com/security/advisories/VMSA-2022-0003.html	A-VMW-CLOU-170222/262
voipmonitor					
voipmonitor					
Improper Privilege Management	04-Feb-22	7.5	An incorrect check in the component cdr.php of Voipmonitor GUI before v24.96 allows unauthenticated attackers to escalate privileges via a crafted request. **CVE ID : CVE-2022-24259**	https://www.voipmonitor.org/changelog-gui?major=5	A-VOI-VOIP-170222/263
Improper Neutralization of Special Elements used in an	04-Feb-22	10	A SQL injection vulnerability in Voipmonitor GUI before v24.96 allows attackers to escalate privileges to the Administrator level.	https://www.voipmonitor.org/changelog-gui?major=5	A-VOI-VOIP-170222/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			**CVE ID : CVE-2022-24260**		
N/A	04-Feb-22	6.8	The config restore function of Voipmonitor GUI before v24.96 does not properly check files sent as restore archives, allowing remote attackers to execute arbitrary commands via a crafted file in the web root. **CVE ID : CVE-2022-24262**	https://www.voipmonitor.org/changelog-gui?major=5	A-VOI-VOIP-170222/265
w-zip_project					
w-zip					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Feb-22	7.5	Path Traversal in NPM w-zip prior to 1.0.12. **CVE ID : CVE-2022-0401**	https://huntr.dev/bounties/d93259aa-ad03-43d6-8846-a00b9f58876d, https://github.com/yuda-lyu/w-zip/commit/d7039d034e02fa358e6656565157cedf5fa83288	A-W-Z-W-ZI-170222/266
welaunch					
wordpress_gdpr\\&ccpa					
Improper Neutralization of Input During Web Page Generation	01-Feb-22	4.3	The check_privacy_settings AJAX action of the WordPress GDPR WordPress plugin before 1.9.27, available to both unauthenticated and authenticated users,	N/A	A-WEL-WORD-170222/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			responds with JSON data without an "application/json" content-type. Since an HTML payload isn't properly escaped, it may be interpreted by a web browser led to this endpoint. Javascript code may be executed on a victim's browser. Due to v1.9.26 adding a CSRF check, the XSS is only exploitable against unauthenticated users (as they all share the same nonce) **CVE ID : CVE-2022-0220**		
wire					
wire-webapp					
Improper Removal of Sensitive Information Before Storage or Transfer	04-Feb-22	2.1	Wire webapp is a web client for the wire messaging protocol. In versions prior to 2022-01-27-production.0 expired ephemeral messages were not reliably removed from local chat history of Wire Webapp. In versions before 2022-01-27-production.0 ephemeral messages and assets might still be accessible through the local search functionality. Any attempt to view one of these message in the chat view will then trigger the deletion. This issue only affects locally stored messages. On premise instances of wire-webapp need to be updated to 2022-01-27-production.0, so that	https://github.com/wireapp/wire-webapp/commit/42c9a1edddbdd5d4d8f9a196a98f6fc19bb21741, https://github.com/wireapp/wire-webapp/security/advisories/GHSA-2w3m-ppfg-hg62	A-WIR-WIRE-170222/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			their users are no longer affected. There are no known workarounds for this issue. **CVE ID : CVE-2022-23605**		
wpdeveloper					
essential_addons_for_elementor					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Feb-22	7.5	The Essential Addons for Elementor WordPress plugin before 5.0.5 does not validate and sanitise some template data before it them in include statements, which could allow unauthenticated attackers to perform Local File Inclusion attack and read arbitrary files on the server, this could also lead to RCE via user uploaded files or other LFI to RCE techniques. **CVE ID : CVE-2022-0320**	N/A	A-WPD-ESSE-170222/269
Xerox					
xmpie_ustore					
Exposure of Sensitive Information to an Unauthorized Actor	07-Feb-22	5	XMPie uStore 12.3.7244.0 allows for administrators to generate reports based on raw SQL queries. Since the application ships with default administrative credentials, an attacker may authenticate into the application and exfiltrate sensitive information from the database. **CVE ID : CVE-2022-23320**	http://xmpie.com, https://www.xmpie.com/ustore-release-notes/	A-XER-XMPI-170222/270
Xwiki					
Xwiki					
Improper	09-Feb-22	6.5	XWiki Platform is a generic	https://jira.x	A-XWI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			wiki platform offering runtime services for applications built on top of it. In affected versions it's possible for an unprivileged user to perform a remote code execution by injecting a groovy script in her own profile and by calling the Reset password feature since the feature is performing a save of the user profile with programming rights in the impacted versions of XWiki. The issue has been patched in XWiki 13.1RC1. There are two different possible workarounds, each consisting of modifying the XWiki/ResetPassword page. 1. The Reset password feature can be entirely disabled by deleting the XWiki/ResetPassword page. 2. The script in XWiki/ResetPassword can also be modified or removed: an administrator can replace it with a simple email contact to ask an administrator to reset the password. **CVE ID : CVE-2022-23616**	wiki.org/browse/XWIKI-16661, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-mgjw-2wrp-r535	XWIK-170222/271
Missing Authorization	09-Feb-22	4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit right can copy the content of a page it does not have access to by using it as	https://github.com/xwiki/xwiki-platform/commit/b35ef0edd4f2ff2c974cbeef6b80fcf9b5a4455	A-XWI-XWIK-170222/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template of a new page. This issue has been patched in XWiki 13.2CR1 and 12.10.6. Users are advised to update. There are no known workarounds for this issue. **CVE ID : CVE-2022-23617**	4, https://github.com/xwiki/xwiki-platform/commit/30c52b01559b8ef5ed1035dac7c34aaf805764d5, https://jira.xwiki.org/browse/XWIKI-18430	
URL Redirection to Untrusted Site ('Open Redirect')	09-Feb-22	5.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions there is no protection against URL redirection to untrusted sites, in particular some well known parameters (xredirect) can be used to perform url redirections. This problem has been patched in XWiki 12.10.7 and XWiki 13.3RC1. Users are advised to update. There are no known workarounds for this issue. **CVE ID : CVE-2022-23618**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-jp55-vvmf-63mv, https://github.com/xwiki/xwiki-platform/commit/5251c02080466bf9fb55288f04a37671108f8096, https://jira.xwiki.org/browse/XWIKI-10309	A-XWI-XWIK-170222/273
Weak Password Recovery Mechanism for Forgotten	09-Feb-22	5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's	https://github.com/xwiki/xwiki-platform/security/adviso	A-XWI-XWIK-170222/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Password			possible to guess if a user has an account on the wiki by using the "Forgot your password" form, even if the wiki is closed to guest users. This problem has been patched on XWiki 12.10.9, 13.4.1 and 13.6RC1. Users are advised yo update. There are no known workarounds for this issue. **CVE ID : CVE-2022-23619**	ries/GHSA-35fg-hjcr-j65f, https://jira.xwiki.org/browse/XWIKI-18787, https://github.com/xwiki/xwiki-platform/commit/d8a3cce48e0ac1a0f4a3cea7a19747382d9c9494	
Missing Authorization	09-Feb-22	4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with SCRIPT right can read any file located in the XWiki WAR (for example xwiki.cfg and xwiki.properties) through XWiki#invokeServletAndReturnAsString as `$xwiki.invokeServletAndReturnAsString("/WEB-INF/xwiki.cfg")`. This issue has been patched in XWiki versions 12.10.9, 13.4.3 and 13.7-rc-1. Users are advised to update. The only workaround is to limit SCRIPT right. **CVE ID : CVE-2022-23621**	https://github.com/xwiki/xwiki-platform/commit/df8bd49b5a4d87a427002c6535fb5b1746ff117a, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-2jhm-qp48-hv5j, https://jira.xwiki.org/browse/XWIKI-18870	A-XWI-XWIK-170222/275
Improper Neutralizatio	09-Feb-22	4.3	XWiki Platform is a generic wiki platform offering	https://github.com/xwiki	A-XWI-XWIK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			runtime services for applications built on top of it. In affected versions there is a cross site scripting (XSS) vector in the `registerinline.vm` template related to the `xredirect` hidden field. This template is only used in the following conditions: 1. The wiki must be open to registration for anyone. 2. The wiki must be closed to view for Guest users or more specifically the XWiki.Registration page must be forbidden in View for guest user. A way to obtain the second condition is when administrators checked the "Prevent unregistered users from viewing pages, regardless of the page rights" box in the administration rights. This issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, 13.10.3. There are two main ways for protecting against this vulnerability, the easiest and the best one is by applying a patch in the `registerinline.vm` template, the patch consists in checking the value of the xredirect field to ensure it matches: `<input type="hidden" name="xredirect" value="$escapetool.xml($!request.xredirect)" />`. If for some reason it's not possible to patch this file, another workaround is to ensure	/xwiki-platform/commit/053d957d53f2a543d158f3ab651e390d2728e0b9, https://jira.xwiki.org/browse/XWIKI-19291, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gx6h-936c-vrrr	170222/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"Prevent unregistered users from viewing pages, regardless of the page rights" is not checked in the rights and apply a better right scheme using groups and rights on spaces. **CVE ID : CVE-2022-23622**		
yet_another_stars_rating_project					
yet_another_stars_rating					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Feb-22	4.3	Cross-Site Scripting (XSS) vulnerability discovered in Yasr – Yet Another Stars Rating WordPress plugin (versions <= 2.9.9), vulnerable at parameter 'source'. **CVE ID : CVE-2022-23980**	https://patchstack.com/database/vulnerability/yet-another-stars-rating/wordpress-yasr-yet-another-stars-rating-plugin-2-9-9-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/yet-another-stars-rating/#developers	A-YET-YET_-170222/277
Zimbra					
collaboration					
Improper Neutralization of Input During Web Page	09-Feb-22	4.3	An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories,	A-ZIM-COLL-170222/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document. **CVE ID : CVE-2022-24682**	https://wiki.zimbra.com/wiki/Security_Center, https://blog.zimbra.com/2022/02/hotfix-available-5-feb-for-zero-day-exploit-vulnerability-in-zimbra-8-8-15/	
Hardware					
Advantech					
adam-3600					
Use of Hard-coded Credentials	04-Feb-22	7.5	The affected product has a hardcoded private key available inside the project folder, which may allow an attacker to achieve Web Server login and perform further actions. **CVE ID : CVE-2022-22987**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-02	H-ADV-ADAM-170222/279
elecom					
wrc-300febk-r					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-22	2.9	Cross-site scripting vulnerability in ELECOM LAN router WRC-300FEBK-R firmware v1.13 and earlier allows an attacker on the adjacent network to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-21799**	https://jvn.jp/en/jp/JVN17482543/index.html, https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRC--170222/280
wrh-300bk3					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH--170222/281
wrh-300bk3-s					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH--170222/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**		
wrh-300dr3-s					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH-170222/283
wrh-300lb3-s					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH-170222/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**		
wrh-300pn3-s					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH--170222/285
wrh-300wh3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH--170222/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**		
wrh-300wh3-s					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	H-ELE-WRH--170222/287
wrh-300yg3-s					
Improper Neutralization of Special	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3	https://www.elecom.co.jp/news/secu	H-ELE-WRH--170222/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	rity/20220208-02/	
mediatek					
mt6580					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/289
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**		
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/291
mt6582e					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/292
mt6582h					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT65-170222/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	ruary-2022	
mt6582t					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/294
mt6582w					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/295
mt6582_90					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT65-170222/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	bulletin/February-2022	
mt6589					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/297
mt6589td					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/298
mt6592e					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-	H-MED-MT65-170222/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	security-bulletin/February-2022	
mt6592h					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/300
mt6592t					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/301
mt6592w					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption	https://corp.mediatek.co	H-MED-MT65-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	m/product-security-bulletin/February-2022	170222/302
mt6592_90					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/303
mt6595					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT65-170222/304
mt6731					
Use After	09-Feb-22	4.6	In fb driver, there is a	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	mediatek.com/product-security-bulletin/February-2022	MT67-170222/305
mt6732					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/306
mt6735					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/307
Improper	09-Feb-22	4.6	In Preloader XFLASH, there is	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	mediatek.com/product-security-bulletin/February-2022	MT67-170222/308
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/309
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/310
Out-of-bounds	09-Feb-22	4.6	In power_hal_manager_service,	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	m/product-security-bulletin/February-2022	170222/311
mt6737					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/312
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/313
Improper Restriction of	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT67-

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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	security-bulletin/February-2022	170222/314
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/315
mt6739					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/316
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-170222/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	bulletin/February-2022	
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/318
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/319
Improper Restriction of Operations within the Bounds of a	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/321
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/322
mt6750					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**		
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/324
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/325
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06171705. **CVE ID : CVE-2022-20037**		
mt6750s					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/327
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/328
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20037		
mt6752					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/330
mt6753					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/331
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20036		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/333
mt6755					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/334
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/336
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/337
mt6755s					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/339
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/340
mt6757					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/341
Improper Restriction	09-Feb-22	2.1	In ion driver, there is a possible information	https://corp.mediatek.co	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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	m/product-security-bulletin/February-2022	170222/342
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/343
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/344
mt6757c					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This	https://corp.mediatek.com/product-	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	security-bulletin/February-2022	170222/345
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/346
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/347
mt6757cd					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT67-170222/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	ruary-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/349
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/350
mt6757ch					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/352
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/353
mt6758					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. 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/February-2022	H-MED-MT67-170222/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/355
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/356
mt6761					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06219064. **CVE ID : CVE-2022-20024**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/358
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/359
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/360
Improper Certificate	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	m/product-security-bulletin/February-2022	170222/361
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/362
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/363
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission	https://corp.mediatek.com/product-	H-MED-MT67-170222/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	security-bulletin/February-2022	
mt6762					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/365
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/366
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT67-170222/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	ruary-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/368
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/369
mt6763					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/371
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/372
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/374
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/375
mt6765					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05862991. **CVE ID : CVE-2022-20017**		
Missing Authorizatio n	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp. mediatek.co m/product-security-bulletin/Feb ruary-2022	H-MED-MT67-170222/377
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp. mediatek.co m/product-security-bulletin/Feb ruary-2022	H-MED-MT67-170222/378
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp. mediatek.co m/product-security-bulletin/Feb ruary-2022	H-MED-MT67-170222/379
Out-of-	09-Feb-22	2.1	In camera driver, there is a	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	mediatek.com/product-security-bulletin/February-2022	MT67-170222/380
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/381
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/382
Improper Restriction of	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT67-170222/383

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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	security-bulletin/February-2022	
mt6768					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/384
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/385
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT67-170222/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	ruary-2022	
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/387
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/388
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/390
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/391
mt6769					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20029		
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/393
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/394
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/396
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/397
mt6771					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/398
Out-of-	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	m/product-security-bulletin/February-2022	170222/399
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/400
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/401
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/403
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/404
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
mt6779					
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/406
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/407
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05850708. **CVE ID : CVE-2022-20031**		
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/409
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/410
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/412
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/413
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/414
mt6781					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/415
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/416
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/417
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-170222/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	bulletin/February-2022	
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/419
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/420
Improper Restriction of Operations within the Bounds of a Memory	09-Feb-22	2.1	In ion driver, 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/February-2022	H-MED-MT67-170222/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			User interaction is not needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/422
mt6785					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/423
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150;	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**		
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/425
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/426
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/427
Improper	09-Feb-22	4.6	In Preloader XFLASH, there is	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	mediatek.com/product-security-bulletin/February-2022	MT67-170222/428
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/429
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/430
Improper Restriction of	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT67-170222/431

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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	security-bulletin/February-2022	
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/432
mt6795					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/433
Improper Restriction of Operations	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT67-170222/434

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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	bulletin/February-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/435
mt6797					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/436
Improper Restriction of Operations within the Bounds of a	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT67-170222/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	ruary-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/438
mt6799					
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/439
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/441
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT67-170222/442
mt6833					
Improper Restriction of Operations within the Bounds of a Memory	09-Feb-22	2.1	In ion driver, 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/February-2022	H-MED-MT68-170222/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			needed for exploitation. Patch ID: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/444
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/445
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/447
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/448
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/449
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after	https://corp.mediatek.com/product-	H-MED-MT68-170222/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	security-bulletin/February-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/451
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/452
Improper Restriction of Operations within the Bounds of a Memory	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**		
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/454
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/455
mt6853					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05862991. **CVE ID : CVE-2022-20017**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/457
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/458
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/459
Concurrent	09-Feb-22	1.9	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 information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	mediatek.com/product-security-bulletin/February-2022	MT68-170222/460
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/461
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/462
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-170222/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	bulletin/February-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/464
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/465
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**		
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/467
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/468
mt6853t					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20029		
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/470
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/471
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/472
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds	https://corp.mediatek.com/product-	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	security-bulletin/February-2022	170222/473
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/474
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/475
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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/February-2022	H-MED-MT68-170222/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**		
mt6873					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/477
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/478
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05837793. **CVE ID : CVE-2022-20030**		
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/480
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/481
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/482
Improper Certificate	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	m/product-security-bulletin/February-2022	170222/483
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/484
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/485
Improper Restriction of Operations	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-170222/486

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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	bulletin/February-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/487
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/488
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
mt6875					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/490
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/491
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/493
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/494
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20040		
mt6877					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/496
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/497
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/498
Use After	09-Feb-22	4.6	In fb driver, there is a	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	mediatek.com/product-security-bulletin/February-2022	MT68-170222/499
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/500
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/501
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**		
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/503
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/504
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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/February-2022	H-MED-MT68-170222/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/506
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/507
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mt6880					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/509
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/510
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mt6883					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/512
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/513
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/514
Concurrent Execution using Shared	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This	https://corp.mediatek.com/product-	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	security-bulletin/February-2022	170222/515
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/516
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/517
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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/February-2022	H-MED-MT68-170222/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**		
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/519
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/520
mt6885					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05862991. **CVE ID : CVE-2022-20017**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/522
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/523
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/524
Concurrent	09-Feb-22	1.9	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 information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	mediatek.com/product-security-bulletin/February-2022	MT68-170222/525
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/526
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/527
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-170222/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	bulletin/February-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/529
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/530
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**		
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/532
mt6889					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/533
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05837793. **CVE ID : CVE-2022-20030**		
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/535
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/536
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/537
Improper Restriction	09-Feb-22	2.1	In ion driver, there is a possible information	https://corp.mediatek.co	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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	m/product-security-bulletin/February-2022	170222/538
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/539
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/540
mt6890					
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after	https://corp.mediatek.com/product-	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	security-bulletin/February-2022	170222/541
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/542
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/543
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
mt6891					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/545
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/546
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. 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/February-2022	H-MED-MT68-170222/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/548
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/549
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/551
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/552
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/553
mt6893					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/554
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/555
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/556
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-170222/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	bulletin/February-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/558
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/559
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**		
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/561
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/562
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20037		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/564
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/565
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT68-170222/566
mt8163					
Out-of-	09-Feb-22	2.1	In cmdq driver, there is a	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	mediatek.com/product-security-bulletin/February-2022	MT81-170222/567
mt8167					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/568
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/569
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT81-170222/570

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: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	bulletin/February-2022	
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/571
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/572
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/574
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/575
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/577
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/578
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/579
Missing Authorizatio	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	m/product-security-bulletin/February-2022	170222/580
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/581
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID: ALPS06148177. **CVE ID : CVE-2022-20043**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/582
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT81-170222/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	ruary-2022	
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/584
Missing Release of Memory after Effective Lifetime	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/585
mt8168					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05862991. **CVE ID : CVE-2022-20017**		
Missing Authorizatio n	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp. mediatek.co m/product-security-bulletin/Feb ruary-2022	H-MED-MT81-170222/587
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp. mediatek.co m/product-security-bulletin/Feb ruary-2022	H-MED-MT81-170222/588
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp. mediatek.co m/product-security-bulletin/Feb ruary-2022	H-MED-MT81-170222/589
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information	https://corp. mediatek.co	H-MED-MT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	m/product-security-bulletin/February-2022	170222/590
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/591
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/592
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
mt8173					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/594
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/595
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**		
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/597
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/598
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/600
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/601
mt8175					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/603
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/604
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/605
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-	H-MED-MT81-170222/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	security-bulletin/February-2022	
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/607
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/608
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/610
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/611
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06219150. **CVE ID : CVE-2022-20040**		
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/613
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/614
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID: ALPS06148177. **CVE ID : CVE-2022-20043**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/616
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/617
Missing Release of Memory after Effective Lifetime	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/618
mt8183					
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT81-170222/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	ruary-2022	
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/620
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/621
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/623
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/624
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID: ALPS06148177. **CVE ID : CVE-2022-20043**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/626
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/627
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/628
Missing Release of Memory after Effective	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT81-170222/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Lifetime			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	ruary-2022	
mt8185					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/630
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/631
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/633
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/634
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/636
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT81-170222/637
mt8321					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/639
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/640
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/641
Improper Restriction of Operations within the	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT83-170222/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	ruary-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/643
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/644
mt8362a					
Improper Restriction of Operations within the Bounds of a	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT83-170222/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	ruary-2022	
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/646
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/647
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. 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/February-2022	H-MED-MT83-170222/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**		
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/649
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/650
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/652
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/653
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/654
Improper Restriction of Operations within the	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT83-170222/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	ruary-2022	
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/656
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/657
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**		
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID: ALPS06148177. **CVE ID : CVE-2022-20043**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/659
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/660
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/662
mt8365					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/663
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/664
Out-of-bounds	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-	H-MED-MT83-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	security-bulletin/February-2022	170222/665
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/666
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/667
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/669
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/670
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/672
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/673
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/674
Missing Authorizatio	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT83-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	m/product-security-bulletin/February-2022	170222/675
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/676
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID: ALPS06148177. **CVE ID : CVE-2022-20043**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/677
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT83-170222/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	ruary-2022	
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/679
Missing Release of Memory after Effective Lifetime	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/680
mt8385					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05862991. **CVE ID : CVE-2022-20017**		
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/682
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/683
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/685
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/686
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/687
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT83-170222/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	bulletin/February-2022	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/689
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/690
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/692
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/693
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06148177; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06148177. **CVE ID : CVE-2022-20043**		
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/695
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/696
Missing Release of Memory after Effective Lifetime	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT83-170222/697
mt8735b					
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read	https://corp.mediatek.co	H-MED-MT87-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	m/product-security-bulletin/February-2022	170222/698
mt8765					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/699
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/700
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/Feb	H-MED-MT87-170222/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	ruary-2022	
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/702
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/703
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06171705. **CVE ID : CVE-2022-20037**		
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/705
mt8766					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/706
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS06219064. **CVE ID : CVE-2022-20024**		
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/708
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/709
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/710
Improper Restriction	09-Feb-22	2.1	In ion driver, there is a possible information	https://corp.mediatek.co	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 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	m/product-security-bulletin/February-2022	170222/711
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/712
mt8768					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/713
Missing Authorizatio	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission	https://corp.mediatek.com/product-	H-MED-MT87-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	security-bulletin/February-2022	170222/714
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/715
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/716
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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/February-2022	H-MED-MT87-170222/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/718
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/719
mt8786					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**		
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/721
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/722
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/723
Improper	09-Feb-22	2.1	In ion driver, there is a	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	mediatek.com/product-security-bulletin/February-2022	MT87-170222/724
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/725
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/726
mt8788					
Improper Restriction	09-Feb-22	2.1	In ion driver, there is a possible information	https://corp.mediatek.co	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 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	m/product-security-bulletin/February-2022	170222/727
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/728
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/729
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/731
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/732
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
mt8789					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/734
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/735
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID:	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05837793. **CVE ID : CVE-2022-20030**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/737
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/738
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/739
Improper Restriction	09-Feb-22	2.1	In ion driver, there is a possible information	https://corp.mediatek.co	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 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	m/product-security-bulletin/February-2022	170222/740
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/741
mt8791					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/742
Missing Authorizatio	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission	https://corp.mediatek.com/product-	H-MED-MT87-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	security-bulletin/February-2022	170222/743
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/744
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/745
Concurrent Execution using Shared Resource with Improper Synchronizat	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion ('Race Condition')			not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**		
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/747
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/748
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/750
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/751
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/752
mt8797					
Improper Restriction of	09-Feb-22	2.1	In ion driver, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT87-

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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	security-bulletin/February-2022	170222/753
Missing Authorization	09-Feb-22	4.6	In system service, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/754
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/755
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/757
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/758
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/760
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/761
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**	https://corp.mediatek.com/product-security-bulletin/February-2022	H-MED-MT87-170222/762
Phoenixcontact					
fl_switch_2005					
Improper	02-Feb-22	9	In Phoenix Contact FL	https://cert.	H-PHO-FL_S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	vde.com/en/advisories/VDE-2022-001/	170222/763
fl_switch_2008					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/764
fl_switch_2008f					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/765
fl_switch_2016					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/766
fl_switch_2105					
Improper Privilege	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in	https://cert.vde.com/en/	H-PHO-FL_S-170222/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	advisories/VDE-2022-001/	
fl_switch_2108					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/768
fl_switch_2116					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/769
fl_switch_2204-2tc-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/770
fl_switch_2205					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect	https://cert.vde.com/en/advisories/V	H-PHO-FL_S-170222/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	DE-2022-001/	
fl_switch_2206-2fx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/772
fl_switch_2206-2fx_sm					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/773
fl_switch_2206-2fx_sm_st					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/774
fl_switch_2206-2fx_st					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows	https://cert.vde.com/en/advisories/VDE-2022-	H-PHO-FL_S-170222/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	001/	
fl_switch_2206-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/776
fl_switch_2206-2sfx_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/777
fl_switch_2206c-2fx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/778
fl_switch_2207-fx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable full access to the device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2207-fx_sm					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/780
fl_switch_2208					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/781
fl_switch_2208c					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/782
fl_switch_2208_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2212-2tc-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/784
fl_switch_2214-2fx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/785
fl_switch_2214-2fx_sm					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/786
fl_switch_2214-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration.	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22509		
fl_switch_2214-2sfx_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/788
fl_switch_2216					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/789
fl_switch_2216_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/790
fl_switch_2304-2gc-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fl_switch_2306-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/792
fl_switch_2306-2sfp_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/793
fl_switch_2308					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/794
fl_switch_2308_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/795
fl_switch_2312-2gc-2sfp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/796
fl_switch_2314-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/797
fl_switch_2314-2sfp_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/798
fl_switch_2316					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/799
fl_switch_2316\\/k1					
Improper	02-Feb-22	9	In Phoenix Contact FL	https://cert.	H-PHO-FL_S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	vde.com/en/advisories/VDE-2022-001/	170222/800
fl_switch_2316_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/801
fl_switch_2404-2tc-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/802
fl_switch_2406-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/803
fl_switch_2406-2sfx_pn					
Improper Privilege	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in	https://cert.vde.com/en/	H-PHO-FL_S-170222/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	advisories/VDE-2022-001/	
fl_switch_2408					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/805
fl_switch_2408_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/806
fl_switch_2412-2tc-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/807
fl_switch_2414-2sfx					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect	https://cert.vde.com/en/advisories/V	H-PHO-FL_S-170222/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	DE-2022-001/	
fl_switch_2414-2sfx_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/809
fl_switch_2416					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/810
fl_switch_2416_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/811
fl_switch_2504-2gc-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows	https://cert.vde.com/en/advisories/VDE-2022-	H-PHO-FL_S-170222/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	001/	
fl_switch_2506-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/813
fl_switch_2506-2sfp\\/k1					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/814
fl_switch_2506-2sfp_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/815
fl_switch_2508					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable full access to the device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2508\\/k1					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/817
fl_switch_2508_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/818
fl_switch_2512-2gc-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/819
fl_switch_2514-2sfp					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2514-2sfp_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/821
fl_switch_2516					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/822
fl_switch_2516_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/823
fl_switch_2608					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration.	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22509		
fl_switch_2608_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/825
fl_switch_2708					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/826
fl_switch_2708_pn					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	H-PHO-FL_S-170222/827
riconmobile					
s9922l					
Improper Neutralization of Special Elements used in an OS Command ('OS	04-Feb-22	10	The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-01	H-RIC-S992-170222/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			**CVE ID : CVE-2022-0365**		
s9922xl					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-22	10	The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user. **CVE ID : CVE-2022-0365**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-01	H-RIC-S992-170222/829
Schneider-electric					
easergy_p3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Feb-22	8.3	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P3 (All versions prior to V30.205) **CVE ID : CVE-2022-22725**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-04	H-SCH-EASE-170222/830
easergy_p5					
Use of Hard-coded Credentials	04-Feb-22	5.4	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-03	H-SCH-EASE-170222/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101) **CVE ID : CVE-2022-22722**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Feb-22	8.3	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101) **CVE ID : CVE-2022-22723**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-03	H-SCH-EASE-170222/832
Tenda					
ax3					
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetFirewallCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the firewallEn parameter. **CVE ID : CVE-2022-24142**	N/A	H-TEN-AX3-170222/833
Out-of-	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN	N/A	H-TEN-AX3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			and AX12 22.03.01.2_CN was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter. **CVE ID : CVE-2022-24143**		170222/834
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function WanParameterSetting. This vulnerability allows attackers to execute arbitrary commands via the gateway, dns1, and dns2 parameters. **CVE ID : CVE-2022-24144**	N/A	H-TEN-AX3-170222/835
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formWifiBasicSet. This vulnerability allows attackers to cause a Denial of Service (DoS) via the security and security_5g parameters. **CVE ID : CVE-2022-24145**	N/A	H-TEN-AX3-170222/836
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetQosBand. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24146**	N/A	H-TEN-AX3-170222/837
Out-of-bounds	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a	N/A	H-TEN-AX3-170222/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			stack overflow in the function fromAdvSetMacMtuWan. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wanMTU, wanSpeed, cloneType, mac, and serviceName parameters. **CVE ID : CVE-2022-24147**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function mDMZSetCfg. This vulnerability allows attackers to execute arbitrary commands via the dmzIp parameter. **CVE ID : CVE-2022-24148**	N/A	H-TEN-AX3-170222/839
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetWirelessRepeat. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wpapsk_crypto parameter. **CVE ID : CVE-2022-24149**	N/A	H-TEN-AX3-170222/840
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function formSetSafeWanWebMan. This vulnerability allows attackers to execute arbitrary commands via the remoteIp parameter. **CVE ID : CVE-2022-24150**	N/A	H-TEN-AX3-170222/841
Out-of-	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN	N/A	H-TEN-AX3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			was discovered to contain a stack overflow in the function fromSetWifiGusetBasic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the shareSpeed parameter. **CVE ID : CVE-2022-24151**		170222/842
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetRouteStatic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24152**	N/A	H-TEN-AX3-170222/843
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formAddMacfilterRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter. **CVE ID : CVE-2022-24153**	N/A	H-TEN-AX3-170222/844
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetRebootTimer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the rebootTime parameter. **CVE ID : CVE-2022-24154**	N/A	H-TEN-AX3-170222/845
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function setSchedWifi. This	N/A	H-TEN-AX3-170222/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) via the schedStartTime and schedEndTime parameters. **CVE ID : CVE-2022-24155**		
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24156**	N/A	H-TEN-AX3-170222/847
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetMacFilterCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceList parameter. **CVE ID : CVE-2022-24157**	N/A	H-TEN-AX3-170222/848
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetIpMacBind. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24158**	N/A	H-TEN-AX3-170222/849
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetPPTPServer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the startIp and	N/A	H-TEN-AX3-170222/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			endIp parameters. **CVE ID : CVE-2022-24159**		
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetDeviceName. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter. **CVE ID : CVE-2022-24160**	N/A	H-TEN-AX3-170222/851
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function GetParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the mac parameter. **CVE ID : CVE-2022-24161**	N/A	H-TEN-AX3-170222/852
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. **CVE ID : CVE-2022-24162**	N/A	H-TEN-AX3-170222/853
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter. **CVE ID : CVE-2022-24163**	N/A	H-TEN-AX3-170222/854
Tendacn					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
g1					
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsHijackRule parameter. **CVE ID : CVE-2022-24164**	N/A	H-TEN-G1-170222/855
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetQvlanList. This vulnerability allows attackers to execute arbitrary commands via the qvlanIP parameter. **CVE ID : CVE-2022-24165**	N/A	H-TEN-G1-170222/856
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the manualTime parameter. **CVE ID : CVE-2022-24166**	N/A	H-TEN-G1-170222/857
Improper Neutralization of Special Elements used in a Command ('Command	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetDMZ. This vulnerability allows attackers	N/A	H-TEN-G1-170222/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			to execute arbitrary commands via the dmzHost1 parameter. **CVE ID : CVE-2022-24167**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpGroup. This vulnerability allows attackers to execute arbitrary commands via the IPGroupStartIP and IPGroupEndIP parameters. **CVE ID : CVE-2022-24168**	N/A	H-TEN-G1-170222/859
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindAdd. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRule parameter. **CVE ID : CVE-2022-24169**	N/A	H-TEN-G1-170222/860
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpSecTunnel. This vulnerability allows attackers to execute arbitrary commands via the IPsecLocalNet and IPsecRemoteNet parameters. **CVE ID : CVE-2022-24170**	N/A	H-TEN-G1-170222/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetPppoeServer. This vulnerability allows attackers to execute arbitrary commands via the pppoeServerIP, pppoeServerStartIP, and pppoeServerEndIP parameters. **CVE ID : CVE-2022-24171**	N/A	H-TEN-G1-170222/862
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDhcpBindRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the addDhcpRules parameter. **CVE ID : CVE-2022-24172**	N/A	H-TEN-G1-170222/863
g3					
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsHijackRule parameter. **CVE ID : CVE-2022-24164**	N/A	H-TEN-G3-170222/864
Improper Neutralization of Special Elements	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection	N/A	H-TEN-G3-170222/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			vulnerability in the function formSetQvlanList. This vulnerability allows attackers to execute arbitrary commands via the qvlanIP parameter. **CVE ID : CVE-2022-24165**		
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the manualTime parameter. **CVE ID : CVE-2022-24166**	N/A	H-TEN-G3-170222/866
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetDMZ. This vulnerability allows attackers to execute arbitrary commands via the dmzHost1 parameter. **CVE ID : CVE-2022-24167**	N/A	H-TEN-G3-170222/867
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpGroup. This vulnerability allows attackers to execute arbitrary commands via the IPGroupStartIP and IPGroupEndIP parameters.	N/A	H-TEN-G3-170222/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24168		
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindAdd. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRule parameter. **CVE ID : CVE-2022-24169**	N/A	H-TEN-G3-170222/869
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpSecTunnel. This vulnerability allows attackers to execute arbitrary commands via the IPsecLocalNet and IPsecRemoteNet parameters. **CVE ID : CVE-2022-24170**	N/A	H-TEN-G3-170222/870
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetPppoeServer. This vulnerability allows attackers to execute arbitrary commands via the pppoeServerIP, pppoeServerStartIP, and pppoeServerEndIP parameters. **CVE ID : CVE-2022-24171**	N/A	H-TEN-G3-170222/871
Out-of-bounds	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were	N/A	H-TEN-G3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			discovered to contain a stack overflow in the function formAddDhcpBindRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the addDhcpRules parameter. **CVE ID : CVE-2022-24172**		170222/872
Operating System					
Advantech					
adam-3600_firmware					
Use of Hard-coded Credentials	04-Feb-22	7.5	The affected product has a hardcoded private key available inside the project folder, which may allow an attacker to achieve Web Server login and perform further actions. **CVE ID : CVE-2022-22987**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-02	O-ADV-ADAM-180222/873
Apple					
macos					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Feb-22	4.4	Local privilege escalation due to race condition on application startup. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 **CVE ID : CVE-2022-24114**	https://security-advisory.acronis.com/advisories/SEC-3316	O-APP-MACO-180222/874
Improper Verification of Cryptographic Signature	04-Feb-22	4.6	Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Cyber Protect Home Office (macOS)	https://security-advisory.acronis.com/advisories/SEC-3359	O-APP-MACO-180222/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before build 39605, Acronis True Image 2021 (macOS) before build 39287 **CVE ID : CVE-2022-24115**		
Exposure of Sensitive Information to an Unauthorized Actor	09-Feb-22	4.3	The Keybase Clients for macOS and Windows before version 5.9.0 fails to properly remove exploded messages initiated by a user. This can occur if the receiving user switches to a non-chat feature and places the host in a sleep state before the sending user explodes the messages. This could lead to disclosure of sensitive information which was meant to be deleted from a user's filesystem. **CVE ID : CVE-2022-22779**	https://explore.zoom.us/en/trust/security/security-bulletin	O-APP-MACO-180222/876
Centos					
centos					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Feb-22	5	SQL Injection vulnerability discovered in Unified Office Total Connect Now that would allow an attacker to extract sensitive information through a cookie parameter. **CVE ID : CVE-2022-24121**	https://unifiedoffice.com/total-connect-now/	O-CEN-CENT-180222/877
elecom					
wrc-300febk-r_firmware					
Improper Neutralization of Input During Web Page	08-Feb-22	2.9	Cross-site scripting vulnerability in ELECOM LAN router WRC-300FEBK-R firmware v1.13 and earlier allows an attacker on the	https://jvn.jp/en/jp/JVN17482543/index.html, https://ww	O-ELE-WRC--180222/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			adjacent network to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-21799**	w.elecom.co.jp/news/security/20220208-02/	
wrh-300bk3-s_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/879
wrh-300bk3_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**		
wrh-300dr3-s_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/881
wrh-300lb3-s_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**		
wrh-300pn3-s_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/883
wrh-300wh3-s_firmware					
Improper Neutralizatio	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN	https://www.elecom.co.j	O-ELE-WRH--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	p/news/security/20220208-02/	180222/884
wrh-300wh3_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors.	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21173		
wrh-300yg3-s_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Feb-22	8.3	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2022-21173**	https://www.elecom.co.jp/news/security/20220208-02/	O-ELE-WRH--180222/886
Google					
android					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS05862991; Issue ID: ALPS05862991. **CVE ID : CVE-2022-20017**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/887
Missing	09-Feb-22	4.6	In system service, there is a	https://corp.	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219064; Issue ID: ALPS06219064. **CVE ID : CVE-2022-20024**	mediatek.com/product-security-bulletin/February-2022	ANDR-180222/888
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. **CVE ID : CVE-2022-20025**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/889
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. **CVE ID : CVE-2022-20026**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/890
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	O-GOO-ANDR-180222/891

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: ALPS06126826; Issue ID: ALPS06126826. **CVE ID : CVE-2022-20027**	bulletin/February-2022	
Out-of-bounds Write	09-Feb-22	4.6	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. **CVE ID : CVE-2022-20028**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/892
Out-of-bounds Read	09-Feb-22	2.1	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. **CVE ID : CVE-2022-20029**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/893
Out-of-bounds Write	09-Feb-22	4.6	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. **CVE ID : CVE-2022-20030**		
Use After Free	09-Feb-22	4.6	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. **CVE ID : CVE-2022-20031**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/895
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Feb-22	1.9	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. **CVE ID : CVE-2022-20032**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/896
Out-of-bounds Read	09-Feb-22	2.1	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. **CVE ID : CVE-2022-20033**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	09-Feb-22	4.6	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. **CVE ID : CVE-2022-20034**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/898
Use After Free	09-Feb-22	2.1	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. **CVE ID : CVE-2022-20035**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/899
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	2.1	In ion driver, 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: ALPS06171689; Issue ID: ALPS06171689. **CVE ID : CVE-2022-20036**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/900
Improper Restriction	09-Feb-22	2.1	In ion driver, there is a possible information	https://corp.mediatek.co	O-GOO-ANDR-

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: ALPS06171705; Issue ID: ALPS06171705. **CVE ID : CVE-2022-20037**	m/product-security-bulletin/February-2022	180222/901
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335. **CVE ID : CVE-2022-20038**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/902
Integer Overflow or Wraparound	09-Feb-22	4.6	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345. **CVE ID : CVE-2022-20039**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/903
Out-of-bounds Write	09-Feb-22	4.6	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150. **CVE ID : CVE-2022-20040**		
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108596; Issue ID: ALPS06108596. **CVE ID : CVE-2022-20041**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/905
Improper Handling of Exceptional Conditions	09-Feb-22	2.1	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. **CVE ID : CVE-2022-20042**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/906
Missing Authorization	09-Feb-22	4.6	In Bluetooth, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06148177; Issue ID: ALPS06148177. **CVE ID : CVE-2022-20043**		
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814. **CVE ID : CVE-2022-20044**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/908
Use After Free	09-Feb-22	4.6	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820. **CVE ID : CVE-2022-20045**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/909
Missing Release of Memory after Effective Lifetime	09-Feb-22	2.1	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410. **CVE ID : CVE-2022-20046**	https://corp.mediatek.com/product-security-bulletin/February-2022	O-GOO-ANDR-180222/910
Linux					
linux_kernel					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-Feb-22	4.6	SQL Server for Linux Containers Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-23276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23276	O-LIN-LINU-180222/911
Improper Handling of Exceptional Conditions	04-Feb-22	2.1	A vulnerability was found in the Linux kernel's eBPF verifier when handling internal data structures. Internal memory locations could be returned to userspace. A local attacker with the permissions to insert eBPF code to the kernel can use this to leak internal kernel memory details defeating some of the exploit mitigations in place for the kernel. This flaws affects kernel versions < v5.16-rc6 **CVE ID : CVE-2022-0264**	https://bugzilla.redhat.com/show_bug.cgi?id=2041547	O-LIN-LINU-180222/912
Missing Initialization of Resource	04-Feb-22	1.9	An issue was discovered in fs/nfs/dir.c in the Linux kernel before 5.16.5. If an application sets the O_DIRECTORY flag, and tries to open a regular file, nfs_atomic_open() performs a regular lookup. If a regular file is found, ENOTDIR should occur, but the server instead returns uninitialized data in the file descriptor. **CVE ID : CVE-2022-24448**	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ac795161c93699d600db16c1a8cc23a65a1eceaf, https://www.spinics.net/lists/stable/msg531976.html, https://cdn.k	O-LIN-LINU-180222/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.5	
Use After Free	04-Feb-22	2.1	A use-after-free vulnerability was found in rtsx_usb_ms_drv_remove in drivers/memstick/host/rtsx_usb_ms.c in memstick in the Linux kernel. In this flaw, a local attacker with a user privilege may impact system Confidentiality. This flaw affects kernel versions prior to 5.14 rc1. **CVE ID : CVE-2022-0487**	https://bugzilla.redhat.com/show_bug.cgi?id=2044561, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=42933c8aa14be1caa9eda41f65cde8a3a95d3e39	O-LIN-LINU-180222/914
Exposure of Resource to Wrong Sphere	02-Feb-22	5.8	NVIDIA Omniverse Launcher contains a Cross-Origin Resource Sharing (CORS) vulnerability which can allow an unprivileged remote attacker, if they can get user to browse malicious site, to acquire access tokens allowing them to access resources in other security domains, which may lead to code execution, escalation of privileges, and impact to confidentiality and integrity. **CVE ID : CVE-2022-21817**	https://nvidia.custhelp.com/app/answers/detail/a_id/5318	O-LIN-LINU-180222/915
Microsoft					
windows					
N/A	01-Feb-22	5	Docker Desktop before 4.4.4 on Windows allows attackers	https://docs.docker.com/	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to move arbitrary files. **CVE ID : CVE-2022-23774**	docker-for-windows/release-notes/	180222/916
Out-of-bounds Read	04-Feb-22	3.6	A security out-of-bounds read information disclosure vulnerability in Trend Micro Worry-Free Business Security Server could allow a local attacker to send garbage data to a specific named pipe and crash the server. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-23805**	https://success.trendmicro.com/solution/000290416	O-MIC-WIND-180222/917
Incorrect Default Permissions	04-Feb-22	4.6	Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 **CVE ID : CVE-2022-24113**	https://security-advisory.acronis.com/advisories/SEC-2881	O-MIC-WIND-180222/918
Exposure of Resource to Wrong Sphere	02-Feb-22	5.8	NVIDIA Omniverse Launcher contains a Cross-Origin Resource Sharing (CORS) vulnerability which can allow an unprivileged remote attacker, if they can get user to browse malicious site, to acquire access tokens	https://nvidia.custhelp.com/app/answers/detail/a_id/5318	O-MIC-WIND-180222/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowing them to access resources in other security domains, which may lead to code execution, escalation of privileges, and impact to confidentiality and integrity. **CVE ID : CVE-2022-21817**		
Exposure of Sensitive Information to an Unauthorized Actor	09-Feb-22	4.3	The Keybase Clients for macOS and Windows before version 5.9.0 fails to properly remove exploded messages initiated by a user. This can occur if the receiving user switches to a non-chat feature and places the host in a sleep state before the sending user explodes the messages. This could lead to disclosure of sensitive information which was meant to be deleted from a user's filesystem. **CVE ID : CVE-2022-22779**	https://explore.zoom.us/en/trust/security/security-bulletin	O-MIC-WIND-180222/920
windows_10					
N/A	09-Feb-22	9.3	Windows Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21971	O-MIC-WIND-180222/921
N/A	09-Feb-22	9.3	Roaming Security Rights Management Services Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21974	O-MIC-WIND-180222/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/923
N/A	09-Feb-22	6	Windows DNS Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21984	O-MIC-WIND-180222/924
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/925
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/926
N/A	09-Feb-22	9.3	Windows Mobile Device Management Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21992	O-MIC-WIND-180222/927
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180222/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21993	guidance/advisory/CVE-2022-21993	
Improper Privilege Management	09-Feb-22	7.2	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21994	O-MIC-WIND-180222/929
N/A	09-Feb-22	6.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21995	O-MIC-WIND-180222/930
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/931
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998	O-MIC-WIND-180222/932
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/934
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/935
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/936
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/937
Uncontrolled Resource Consumption	09-Feb-22	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-22712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22712	O-MIC-WIND-180222/938
Improper Privilege Management	09-Feb-22	7.2	Named Pipe File System Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22715**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180222/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2022-22715	
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/940
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/941
windows_11					
N/A	09-Feb-22	9.3	Windows Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21971	O-MIC-WIND-180222/942
N/A	09-Feb-22	9.3	Roaming Security Rights Management Services Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21974	O-MIC-WIND-180222/943
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180222/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2022-21981	
N/A	09-Feb-22	6	Windows DNS Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21984	O-MIC-WIND-180222/945
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/946
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/947
N/A	09-Feb-22	9.3	Windows Mobile Device Management Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21992	O-MIC-WIND-180222/948
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/949
Improper Privilege Management	09-Feb-22	7.2	Windows DWM Core Library Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180222/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21994	-US/security-guidance/advisory/CVE-2022-21994	
N/A	09-Feb-22	6.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21995	O-MIC-WIND-180222/951
Improper Privilege Management	09-Feb-22	7.2	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21996	O-MIC-WIND-180222/952
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/953
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998	O-MIC-WIND-180222/954
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21999		
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/956
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/957
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/958
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/959
Uncontrolled Resource Consumption	09-Feb-22	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-22712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22712	O-MIC-WIND-180222/960
Improper Privilege Management	09-Feb-22	7.2	Named Pipe File System Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180222/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22715	-US/security-guidance/advisory/CVE-2022-22715	
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/962
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/963
windows_7					
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/964
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/965
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180222/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2022-21989	
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/967
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998	O-MIC-WIND-180222/968
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/969
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/970
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/971
Uncontrolled	09-Feb-22	4.9	Windows Common Log File	https://port	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	WIND-180222/972
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/973
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/974
windows_8.1					
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/975
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/976
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180222/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				-US/security-guidance/advisory/CVE-2022-21989	
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/978
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/979
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998	O-MIC-WIND-180222/980
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/981
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180222/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2022-22000	
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/983
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/984
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/985
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/986
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/987
windows_rt_8.1					
Improper	09-Feb-22	4.6	Windows Common Log File	https://port	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	WIND-180222/988
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/989
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/990
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/991
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/992
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180222/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2022-21998	
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/994
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/995
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/996
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/997
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/998
Improper Privilege	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	osoft.com/en-US/security-guidance/advisory/CVE-2022-22717	180222/999
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/1000
windows_server					
N/A	09-Feb-22	9.3	Windows Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21971	O-MIC-WIND-180222/1001
N/A	09-Feb-22	9.3	Roaming Security Rights Management Services Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21974	O-MIC-WIND-180222/1002
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/1003
N/A	09-Feb-22	6	Windows DNS Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21984**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180222/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2022-21984	
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/1005
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/1006
N/A	09-Feb-22	9.3	Windows Mobile Device Management Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21992	O-MIC-WIND-180222/1007
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/1008
Improper Privilege Management	09-Feb-22	7.2	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21994	O-MIC-WIND-180222/1009
N/A	09-Feb-22	6.8	Windows Hyper-V Remote	https://port	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. **CVE ID : CVE-2022-21995**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21995	WIND-180222/1010
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/1011
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998	O-MIC-WIND-180222/1012
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/1013
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/1014
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180222/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22001	visory/CVE-2022-22001	
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/1016
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/1017
Uncontrolled Resource Consumption	09-Feb-22	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-22712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22712	O-MIC-WIND-180222/1018
Improper Privilege Management	09-Feb-22	7.2	Named Pipe File System Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22715**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22715	O-MIC-WIND-180222/1019
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/1020
Improper Privilege	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	osoft.com/en-US/security-guidance/advisory/CVE-2022-22718	180222/1021
windows_server_2008					
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/1022
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/1023
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/1024
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/1025
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180222/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2022-21998	
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/1027
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/1028
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/1029
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/1030
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
windows_server_2012					
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/1032
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/1033
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/1034
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/1035
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/1036
Exposure of Resource to Wrong	09-Feb-22	4.9	Windows Common Log File System Driver Information	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180222/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	-US/security-guidance/advisory/CVE-2022-21998	7
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/1038
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/1039
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/1040
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/1041
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/1043
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/1044
windows_server_2016					
N/A	09-Feb-22	9.3	Roaming Security Rights Management Services Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21974	O-MIC-WIND-180222/1045
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/1046
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985	O-MIC-WIND-180222/1047
Improper Privilege	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability.	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			**CVE ID : CVE-2022-21989**	osoft.com/en-US/security-guidance/advisory/CVE-2022-21989	180222/1048
N/A	09-Feb-22	9.3	Windows Mobile Device Management Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21992	O-MIC-WIND-180222/1049
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/1050
N/A	09-Feb-22	6.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21995	O-MIC-WIND-180222/1051
Improper Privilege Management	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997	O-MIC-WIND-180222/1052
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180222/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2022-21998	
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/1054
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/1055
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/1056
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002	O-MIC-WIND-180222/1057
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/1058
Improper Privilege	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is	https://portal.msrc.microsoft.com/en	O-MIC-WIND-180222/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	-US/security-guidance/advisory/CVE-2022-22717	9
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/1060
windows_server_2019					
N/A	09-Feb-22	9.3	Windows Runtime Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21971	O-MIC-WIND-180222/1061
N/A	09-Feb-22	9.3	Roaming Security Rights Management Services Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21974	O-MIC-WIND-180222/1062
Improper Privilege Management	09-Feb-22	4.6	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22000. **CVE ID : CVE-2022-21981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981	O-MIC-WIND-180222/1063
Exposure of Resource to Wrong Sphere	09-Feb-22	2.1	Windows Remote Access Connection Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-21985**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-180222/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2022-21985	
Improper Privilege Management	09-Feb-22	6.9	Windows Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989	O-MIC-WIND-180222/1065
N/A	09-Feb-22	9.3	Windows Mobile Device Management Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21992	O-MIC-WIND-180222/1066
Exposure of Resource to Wrong Sphere	09-Feb-22	7.8	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993	O-MIC-WIND-180222/1067
Improper Privilege Management	09-Feb-22	7.2	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-21994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21994	O-MIC-WIND-180222/1068
N/A	09-Feb-22	6.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-21995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21995	O-MIC-WIND-180222/1069
Improper Privilege	09-Feb-22	3.6	Windows Print Spooler Elevation of Privilege	https://portal.msrc.micr	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Vulnerability. This CVE ID is unique from CVE-2022-21999, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21997**	osoft.com/en-US/security-guidance/advisory/CVE-2022-21997	180222/1070
Exposure of Resource to Wrong Sphere	09-Feb-22	4.9	Windows Common Log File System Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-21998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998	O-MIC-WIND-180222/1071
Improper Privilege Management	09-Feb-22	4.6	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-22717, CVE-2022-22718. **CVE ID : CVE-2022-21999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999	O-MIC-WIND-180222/1072
Improper Privilege Management	09-Feb-22	7.2	Windows Common Log File System Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21981. **CVE ID : CVE-2022-22000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000	O-MIC-WIND-180222/1073
Improper Privilege Management	09-Feb-22	7.2	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001	O-MIC-WIND-180222/1074
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows User Account Profile Picture Denial of Service Vulnerability. **CVE ID : CVE-2022-22002**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-180222/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2022-22002	
Uncontrolled Resource Consumption	09-Feb-22	4.9	Windows Common Log File System Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-22710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710	O-MIC-WIND-180222/1076
Uncontrolled Resource Consumption	09-Feb-22	4.7	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-22712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22712	O-MIC-WIND-180222/1077
Improper Privilege Management	09-Feb-22	7.2	Named Pipe File System Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-22715**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22715	O-MIC-WIND-180222/1078
Improper Privilege Management	09-Feb-22	6.9	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22718. **CVE ID : CVE-2022-22717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717	O-MIC-WIND-180222/1079
Improper Privilege Management	09-Feb-22	7.2	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21997, CVE-2022-21999, CVE-2022-22717. **CVE ID : CVE-2022-22718**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718	O-MIC-WIND-180222/1080
Phoenixcontact					
fl_switch_2005_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1081
fl_switch_2008f_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1082
fl_switch_2008_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1083
fl_switch_2016_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1084
fl_switch_2105_firmware					
Improper	02-Feb-22	9	In Phoenix Contact FL	https://cert.	O-PHO-FL_S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	vde.com/en/advisories/VDE-2022-001/	180222/1085
fl_switch_2108_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1086
fl_switch_2116_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1087
fl_switch_2204-2tc-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1088
fl_switch_2205_firmware					
Improper Privilege	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in	https://cert.vde.com/en/	O-PHO-FL_S-180222/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	advisories/VDE-2022-001/	9
fl_switch_2206-2fx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1090
fl_switch_2206-2fx_sm_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1091
fl_switch_2206-2fx_sm_st_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1092
fl_switch_2206-2fx_st_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect	https://cert.vde.com/en/advisories/V	O-PHO-FL_S-180222/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	DE-2022-001/	
fl_switch_2206-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1094
fl_switch_2206-2sfx_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1095
fl_switch_2206c-2fx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1096
fl_switch_2207-fx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows	https://cert.vde.com/en/advisories/VDE-2022-	O-PHO-FL_S-180222/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	001/	
fl_switch_2207-fx_sm_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1098
fl_switch_2208c_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1099
fl_switch_2208_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1100
fl_switch_2208_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable full access to the device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2212-2tc-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1102
fl_switch_2214-2fx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1103
fl_switch_2214-2fx_sm_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1104
fl_switch_2214-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2214-2sfx_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1106
fl_switch_2216_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1107
fl_switch_2216_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1108
fl_switch_2304-2gc-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration.	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22509		
fl_switch_2306-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1110
fl_switch_2306-2sfp_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1111
fl_switch_2308_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1112
fl_switch_2308_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fl_switch_2312-2gc-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1114
fl_switch_2314-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1115
fl_switch_2314-2sfp_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1116
fl_switch_2316\\/k1_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1117
fl_switch_2316_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1118
fl_switch_2316_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1119
fl_switch_2404-2tc-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1120
fl_switch_2406-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1121
fl_switch_2406-2sfx_pn_firmware					
Improper	02-Feb-22	9	In Phoenix Contact FL	https://cert.	O-PHO-FL_S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	vde.com/en/advisories/VDE-2022-001/	180222/1122
fl_switch_2408_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1123
fl_switch_2408_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1124
fl_switch_2412-2tc-2sfx_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1125
fl_switch_2414-2sfx_firmware					
Improper Privilege	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in	https://cert.vde.com/en/	O-PHO-FL_S-180222/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	advisories/VDE-2022-001/	6
fl_switch_2414-2sfx_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1127
fl_switch_2416_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1128
fl_switch_2416_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1129
fl_switch_2504-2gc-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect	https://cert.vde.com/en/advisories/V	O-PHO-FL_S-180222/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	DE-2022-001/	
fl_switch_2506-2sfp\\/k1_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1131
fl_switch_2506-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1132
fl_switch_2506-2sfp_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1133
fl_switch_2508\\/k1_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows	https://cert.vde.com/en/advisories/VDE-2022-	O-PHO-FL_S-180222/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	001/	
fl_switch_2508_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1135
fl_switch_2508_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1136
fl_switch_2512-2gc-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1137
fl_switch_2514-2sfp_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable full access to the device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2514-2sfp_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1139
fl_switch_2516_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1140
fl_switch_2516_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1141
fl_switch_2608_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device configuration. **CVE ID : CVE-2022-22509**		
fl_switch_2608_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1143
fl_switch_2708_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1144
fl_switch_2708_pn_firmware					
Improper Privilege Management	02-Feb-22	9	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration. **CVE ID : CVE-2022-22509**	https://cert.vde.com/en/advisories/VDE-2022-001/	O-PHO-FL_S-180222/1145
Redhat					
enterprise_linux					
Use After Free	04-Feb-22	2.1	A use-after-free vulnerability was found in rtsx_usb_ms_drv_remove in drivers/memstick/host/rtsx_usb_ms.c in memstick in the Linux kernel. In this flaw, a	https://bugzilla.redhat.com/show_bug.cgi?id=2044561, https://git.k	O-RED-ENTE-180222/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attacker with a user privilege may impact system Confidentiality. This flaw affects kernel versions prior to 5.14 rc1. **CVE ID : CVE-2022-0487**	ernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=42933c8aa14be1caa9eda41f65cde8a3a95d3e39	
riconmobile					
s9922l_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-22	10	The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user. **CVE ID : CVE-2022-0365**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-01	O-RIC-S992-180222/1147
s9922xl_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-22	10	The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user. **CVE ID : CVE-2022-0365**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-01	O-RIC-S992-180222/1148
Schneider-electric					
easergy_p3_firmware					
Buffer Copy without Checking Size of Input ('Classic	04-Feb-22	8.3	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program	https://download.schneider-electric.com/files?p_Doc_R	O-SCH-EASE-180222/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P3 (All versions prior to V30.205) **CVE ID : CVE-2022-22725**	ef=SEVD-2022-011-04	
easergy_p5_firmware					
Use of Hard-coded Credentials	04-Feb-22	5.4	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101) **CVE ID : CVE-2022-22722**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-03	O-SCH-EASE-180222/1150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Feb-22	8.3	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-03	O-SCH-EASE-180222/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tripping function via GOOSE can be impacted. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101) **CVE ID : CVE-2022-22723**		
Tenda					
ax3_firmware					
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetFirewallCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the firewallEn parameter. **CVE ID : CVE-2022-24142**	N/A	O-TEN-AX3_-180222/1152
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN and AX12 22.03.01.2_CN was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter. **CVE ID : CVE-2022-24143**	N/A	O-TEN-AX3_-180222/1153
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function WanParameterSetting. This vulnerability allows attackers to execute arbitrary commands via the gateway, dns1, and dns2 parameters. **CVE ID : CVE-2022-24144**	N/A	O-TEN-AX3_-180222/1154
Out-of-	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN	N/A	O-TEN-AX3_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			was discovered to contain a stack overflow in the function formWifiBasicSet. This vulnerability allows attackers to cause a Denial of Service (DoS) via the security and security_5g parameters. **CVE ID : CVE-2022-24145**		180222/1155
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetQosBand. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24146**	N/A	O-TEN-AX3_-180222/1156
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromAdvSetMacMtuWan. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wanMTU, wanSpeed, cloneType, mac, and serviceName parameters. **CVE ID : CVE-2022-24147**	N/A	O-TEN-AX3_-180222/1157
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function mDMZSetCfg. This vulnerability allows attackers to execute arbitrary commands via the dmzIp parameter. **CVE ID : CVE-2022-24148**	N/A	O-TEN-AX3_-180222/1158
Out-of-bounds	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a	N/A	O-TEN-AX3_-180222/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			stack overflow in the function fromSetWirelessRepeat. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wpapsk_crypto parameter. **CVE ID : CVE-2022-24149**		9
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function formSetSafeWanWebMan. This vulnerability allows attackers to execute arbitrary commands via the remoteIp parameter. **CVE ID : CVE-2022-24150**	N/A	O-TEN-AX3_-180222/1160
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetWifiGusetBasic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the shareSpeed parameter. **CVE ID : CVE-2022-24151**	N/A	O-TEN-AX3_-180222/1161
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetRouteStatic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24152**	N/A	O-TEN-AX3_-180222/1162
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formAddMacfilterRule. This	N/A	O-TEN-AX3_-180222/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter. **CVE ID : CVE-2022-24153**		
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetRebootTimer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the rebootTime parameter. **CVE ID : CVE-2022-24154**	N/A	O-TEN-AX3_-180222/1164
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function setSchedWifi. This vulnerability allows attackers to cause a Denial of Service (DoS) via the schedStartTime and schedEndTime parameters. **CVE ID : CVE-2022-24155**	N/A	O-TEN-AX3_-180222/1165
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24156**	N/A	O-TEN-AX3_-180222/1166
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetMacFilterCfg. This vulnerability allows attackers to cause a Denial of Service	N/A	O-TEN-AX3_-180222/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) via the deviceList parameter. **CVE ID : CVE-2022-24157**		
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetIpMacBind. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. **CVE ID : CVE-2022-24158**	N/A	O-TEN-AX3_-180222/1168
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetPPTPServer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the startIp and endIp parameters. **CVE ID : CVE-2022-24159**	N/A	O-TEN-AX3_-180222/1169
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetDeviceName. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter. **CVE ID : CVE-2022-24160**	N/A	O-TEN-AX3_-180222/1170
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function GetParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the mac parameter. **CVE ID : CVE-2022-24161**	N/A	O-TEN-AX3_-180222/1171
Out-of-	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN	N/A	O-TEN-AX3_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. **CVE ID : CVE-2022-24162**		180222/1172
Out-of-bounds Write	04-Feb-22	7.8	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter. **CVE ID : CVE-2022-24163**	N/A	O-TEN-AX3_-180222/1173
Tendacn					
g1_firmware					
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsHijackRule parameter. **CVE ID : CVE-2022-24164**	N/A	O-TEN-G1_F-180222/1174
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetQvlanList. This vulnerability allows attackers to execute arbitrary commands via the qvlanIP parameter.	N/A	O-TEN-G1_F-180222/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24165		
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the manualTime parameter. **CVE ID : CVE-2022-24166**	N/A	O-TEN-G1_F-180222/1176
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetDMZ. This vulnerability allows attackers to execute arbitrary commands via the dmzHost1 parameter. **CVE ID : CVE-2022-24167**	N/A	O-TEN-G1_F-180222/1177
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpGroup. This vulnerability allows attackers to execute arbitrary commands via the IPGroupStartIP and IPGroupEndIP parameters. **CVE ID : CVE-2022-24168**	N/A	O-TEN-G1_F-180222/1178
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindAdd. This	N/A	O-TEN-G1_F-180222/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRule parameter. **CVE ID : CVE-2022-24169**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpSecTunnel. This vulnerability allows attackers to execute arbitrary commands via the IPsecLocalNet and IPsecRemoteNet parameters. **CVE ID : CVE-2022-24170**	N/A	O-TEN-G1_F-180222/1180
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetPppoeServer. This vulnerability allows attackers to execute arbitrary commands via the pppoeServerIP, pppoeServerStartIP, and pppoeServerEndIP parameters. **CVE ID : CVE-2022-24171**	N/A	O-TEN-G1_F-180222/1181
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDhcpBindRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the addDhcpRules	N/A	O-TEN-G1_F-180222/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter. **CVE ID : CVE-2022-24172**		
g3_firmware					
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsHijackRule parameter. **CVE ID : CVE-2022-24164**	N/A	O-TEN-G3_F-180222/1183
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetQvlanList. This vulnerability allows attackers to execute arbitrary commands via the qvlanIP parameter. **CVE ID : CVE-2022-24165**	N/A	O-TEN-G3_F-180222/1184
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the manualTime parameter. **CVE ID : CVE-2022-24166**	N/A	O-TEN-G3_F-180222/1185
Improper Neutralization of Special Elements	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection	N/A	O-TEN-G3_F-180222/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			vulnerability in the function formSetDMZ. This vulnerability allows attackers to execute arbitrary commands via the dmzHost1 parameter. **CVE ID : CVE-2022-24167**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpGroup. This vulnerability allows attackers to execute arbitrary commands via the IPGroupStartIP and IPGroupEndIP parameters. **CVE ID : CVE-2022-24168**	N/A	O-TEN-G3_F-180222/1187
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindAdd. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRule parameter. **CVE ID : CVE-2022-24169**	N/A	O-TEN-G3_F-180222/1188
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpSecTunnel. This vulnerability allows attackers to execute arbitrary commands via the IPsecLocalNet and	N/A	O-TEN-G3_F-180222/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPsecRemoteNet parameters. **CVE ID : CVE-2022-24170**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-22	7.5	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetPppoeServer. This vulnerability allows attackers to execute arbitrary commands via the pppoeServerIP, pppoeServerStartIP, and pppoeServerEndIP parameters. **CVE ID : CVE-2022-24171**	N/A	O-TEN-G3_F-180222/1190
Out-of-bounds Write	04-Feb-22	7.8	Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDhcpBindRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the addDhcpRules parameter. **CVE ID : CVE-2022-24172**	N/A	O-TEN-G3_F-180222/1191
Vmware					
cloud_foundation					
Insertion of Sensitive Information into Log File	04-Feb-22	4	VMware Cloud Foundation contains an information disclosure vulnerability due to logging of credentials in plain-text within multiple log files on the SDDC Manager. A malicious actor with root access on VMware Cloud Foundation SDDC Manager may be able to view	https://www.vmware.com/security/advisories/VMSA-2022-0003.html	O-VMW-CLOU-180222/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials in plaintext within one or more log files. **CVE ID : CVE-2022-22939**		