National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Jun 2022 Vol. 09 No. 11

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 2code					
Product: ask_me					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-22	6.1	The Ask me WordPress theme before 6.8.2 does not properly sanitise and escape several of the fields in the Edit Profile page, leading to Reflected Cross-Site Scripting issues **CVE ID : CVE-2022-1241**	N/A	A-2CO-ASK_-200622/1
Cross-Site Request Forgery (CSRF)	08-Jun-22	6.5	The Ask me WordPress theme before 6.8.2 does not perform CSRF checks for any of its AJAX actions, allowing an attacker to trick logged in users to perform various actions on their behalf on the site. **CVE ID : CVE-2022-1424**	N/A	A-2CO-ASK_-200622/2
Product: discy					
Cross-Site Request Forgery (CSRF)	08-Jun-22	4.3	The Discy WordPress theme before 5.2 lacks CSRF checks in some AJAX actions, allowing an attacker to make a logged in admin change arbitrary 's settings including payment methods via a CSRF attack	N/A	A-2CO-DISC-200622/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1421		
Cross-Site Request Forgery (CSRF)	08-Jun-22	6.5	The Discy WordPress theme before 5.2 does not check for CSRF tokens in the AJAX action discy_reset_options, allowing an attacker to trick an admin into resetting the site settings back to defaults. **CVE ID : CVE-2022-1422**	N/A	A-2CO-DISC-200622/4
Product: wpqa_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-22	6.1	The WPQA Builder WordPress plugin before 5.4, used as a companion for the Discy and Himer , does not sanitise and escape a parameter on its reset password form which makes it possible to perform Reflected Cross-Site Scripting attacks **CVE ID : CVE-2022-1597**	N/A	A-2CO-WPQA-200622/5
Vendor: ABB					
Product: e-design					
Incorrect Default Permissions	02-Jun-22	7.8	Incorrect Default Permissions vulnerability in ABB e-Design allows attacker to install malicious software executing with SYSTEM permissions violating	https://search.abb.com/library/Download.aspx?DocumentID=2%20CMT%200%200%206%200%208%206&LanguageCode=en&DocumentP	A-ABB-E-DE-200622/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability of the target machine. **CVE ID : CVE-2022-28702**	artId=&Action=Launch	
Incorrect Default Permissions	02-Jun-22	7.8	Incorrect Default Permissions vulnerability in ABB e-Design allows attacker to install malicious software executing with SYSTEM permissions violating confidentiality, integrity, and availability of the target machine. **CVE ID : CVE-2022-29483**	https://search.abb.com/library/Download.aspx?DocumentID=2%20CMT%200%200%206%200%208%206&LanguageCode=en&DocumentPartId=&Action=Launch	A-ABB-E-DE-200622/7
Vendor: aceware					
Product: aceweb_online_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	ACEweb Online Portal 3.5.065 was discovered to contain a cross-site scripting (XSS) vulnerability via the txtNmName1 parameter in person.awp. **CVE ID : CVE-2022-24238**	https://www.aceware.com/forum/viewtopic.php?f=7&t=481	A-ACE-ACEW-200622/8
Unrestricted Upload of File with Dangerous Type	02-Jun-22	9.8	ACEweb Online Portal 3.5.065 was discovered to contain an unrestricted file upload vulnerability via attachments.awp. **CVE ID : CVE-2022-24239**	https://www.aceware.com/forum/viewtopic.php?f=7&t=481	A-ACE-ACEW-200622/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	ACEweb Online Portal 3.5.065 was discovered to contain a SQL injection vulnerability via the criteria parameter in showschedule.awp. **CVE ID : CVE-2022-24240**	https://www.aceware.com/forum/viewtopic.php?f=7&t=481	A-ACE-ACEW-200622/10
Externally Controlled Reference to a Resource in Another Sphere	02-Jun-22	7.5	ACEweb Online Portal 3.5.065 was discovered to contain an External Controlled File Path and Name vulnerability via the txtFilePath parameter in attachments.awp. **CVE ID : CVE-2022-24241**	https://www.aceware.com/forum/viewtopic.php?f=7&t=481	A-ACE-ACEW-200622/11
Unrestricted Upload of File with Dangerous Type	02-Jun-22	7.5	ACEweb Online Portal 3.5.065 allows unauthenticated SMB hash capture via UNC. By specifying the UNC file path of an external SMB share when uploading a file, an attacker can induce the victim server to disclose the username and password hash of the user executing the ACEweb Online software. **CVE ID : CVE-2022-24581**	https://www.aceware.com/forum/viewtopic.php?f=7&t=481	A-ACE-ACEW-200622/12
Vendor: adbyby_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: adbyby					
Allocation of Resources Without Limits or Throttling	03-Jun-22	6.5	adbyby v2.7 allows external users to make connections via port 8118. This can cause a program logic error and lead to a Denial of Service (DoS) via high CPU usage due to a large number of connections. **CVE ID : CVE-2022-29767**	N/A	A-ADB-ADBY-200622/13
Vendor: afian					
Product: filerun					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-22	8.8	In Afian Filerun 20220202, lack of sanitization of the POST parameter "metadata[]" in `/?module=fileman&section=get&page=grid` leads to SQL injection. **CVE ID : CVE-2022-30469**	https://filerun.com/changelog	A-AFI-FILE-200622/14
N/A	02-Jun-22	9.8	In Afian Filerun 20220202 Changing the "search_tika_path" variable to a custom (and previously uploaded) jar file results in remote code execution in the context of the webserver user. **CVE ID : CVE-2022-30470**	https://filerun.com/changelog	A-AFI-FILE-200622/15
Vendor: aleksis					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: aleksis					
Incorrect Authorization	03-Jun-22	6.5	An access control issue in aleksis/core/util/auth_helpers.py: ClientProtectedResourceMixin of AlekSIS-Core v2.8.1 and below allows attackers to access arbitrary scopes if no allowed scopes are specifically set. **CVE ID : CVE-2022-29773**	https://aleksis.org/2022-05-04_advisory.html	A-ALE-ALEK-200622/16
Vendor: Atlassian					
Product: confluence_data_center					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jun-22	9.8	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1. **CVE ID : CVE-2022-26134**	https://jira.atlassian.com/browse/CONFSERVER-79016	A-ATL-CONF-200622/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: confluence_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jun-22	9.8	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1. **CVE ID : CVE-2022-26134**	https://jira.atlassian.com/browse/CONFSERVER-79016	A-ATL-CONF-200622/18
Vendor: badminton_center_management_system_project					
Product: badminton_center_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Badminton Center Management System V1.0 is vulnerable to SQL Injection via parameter 'id' in /bcms/admin/court_rentals/update_status.php. **CVE ID : CVE-2022-30490**	N/A	A-BAD-BADM-200622/19
Improper Neutralization of Special Elements	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page	N/A	A-BAD-BADM-200622/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			=reports/daily_sales_report&date=. **CVE ID : CVE-2022-31985**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=reports/daily_court_rental_report&date=. **CVE ID : CVE-2022-31986**	N/A	A-BAD-BADM-200622/21
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/?page=reports/daily_services_report&date=. **CVE ID : CVE-2022-31988**	N/A	A-BAD-BADM-200622/22
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=user/manage_user&id=. **CVE ID : CVE-2022-31989**	N/A	A-BAD-BADM-200622/23
Improper Neutralization of Special Elements used in an SQL	02-Jun-22	9.8	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/classes/Master.php?f=delete_product.	N/A	A-BAD-BADM-200622/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2022-31990**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/classes/Master.php?f=delete_court. **CVE ID : CVE-2022-31991**	N/A	A-BAD-BADM-200622/25
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=court_rentals/view_court_rental&id=. **CVE ID : CVE-2022-31992**	N/A	A-BAD-BADM-200622/26
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/classes/Master.php?f=delete_service. **CVE ID : CVE-2022-31993**	N/A	A-BAD-BADM-200622/27
Improper Neutralization of Special Elements used in an SQL Command	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=sales/view_details&id. **CVE ID : CVE-2022-31994**	N/A	A-BAD-BADM-200622/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/?page=sales/manage_sale&id=. **CVE ID : CVE-2022-31996**	N/A	A-BAD-BADM-200622/29
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=service_transactions/view_details&id=. **CVE ID : CVE-2022-31998**	N/A	A-BAD-BADM-200622/30
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=service_transactions/manage_service_transaction&id=. **CVE ID : CVE-2022-32000**	N/A	A-BAD-BADM-200622/31
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/products/view_product.php?id=. **CVE ID : CVE-2022-32001**	N/A	A-BAD-BADM-200622/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/courts/manage_court.php?id=. **CVE ID : CVE-2022-32002**	N/A	A-BAD-BADM-200622/33
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/courts/view_court.php?id=. **CVE ID : CVE-2022-32003**	N/A	A-BAD-BADM-200622/34
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/products/manage_product.php?id=. **CVE ID : CVE-2022-32004**	N/A	A-BAD-BADM-200622/35
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/services/manage_service.php?id=. **CVE ID : CVE-2022-32005**	N/A	A-BAD-BADM-200622/36
Improper Neutralization of	02-Jun-22	7.2	Badminton Center Management System v1.0 is vulnerable to	N/A	A-BAD-BADM-200622/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			SQL Injection via /bcms/admin/services/view_service.php?id=. **CVE ID : CVE-2022-32006**		
Vendor: Barco					
Product: control_room_management_suite					
Improper Authentication	02-Jun-22	5.3	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload mechanism. This upload can be executed without authentication. **CVE ID : CVE-2022-26971**	https://www.barco.com/en/support/transform-n-management-server, https://www.barco.com/en/support/knowledge-base/KB12681	A-BAR-CONT-200622/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a URL /cgi-bin endpoint. The URL parameters are not correctly sanitized, leading to reflected XSS. **CVE ID : CVE-2022-26972**	https://www.barco.com/en/support/transform-n-management-server, https://www.barco.com/en/support/knowledge-base/KB12685	A-BAR-CONT-200622/39
Generation of Error Message Containing Sensitive	02-Jun-22	5.3	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a	https://www.barco.com/en/support/knowledge-base/KB12678, https://www.b	A-BAR-CONT-200622/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			license file upload mechanism. By tweaking the license file name, the returned error message exposes internal directory path details. **CVE ID : CVE-2022-26973**	arco.com/en/support/transform-n-management-server	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a file upload mechanism. Lack of input sanitization in the upload mechanism leads to reflected XSS. **CVE ID : CVE-2022-26974**	https://www.barco.com/en/support/transform-n-management-server, https://www.barco.com/en/support/knowledge-base/KB12684	A-BAR-CONT-200622/41
Improper Authentication	02-Jun-22	7.5	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing log files without authentication. **CVE ID : CVE-2022-26975**	https://www.barco.com/en/support/knowledge-base/KB12677, https://www.barco.com/en/support/transform-n-management-server	A-BAR-CONT-200622/42
Improper Neutralization of Input During Web Page Generation	02-Jun-22	5.4	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload	https://www.barco.com/en/support/transform-n-management-server, https://www.b	A-BAR-CONT-200622/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			mechanism. Lack of input sanitization in the upload mechanism is leads to reflected XSS. **CVE ID : CVE-2022-26976**	arco.com/en/support/knowledge-base/KB12682	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload mechanism. Lack of input sanitization of the upload mechanism is leads to stored XSS. **CVE ID : CVE-2022-26977**	https://www.barco.com/en/support/transform-n-management-server, https://www.barco.com/en/support/knowledge-base/KB12683	A-BAR-CONT-200622/44
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a URL /checklogin.jsp endpoint. The os_username parameters is not correctly sanitized, leading to reflected XSS. **CVE ID : CVE-2022-26978**	https://www.barco.com/en/support/transform-n-management-server, https://www.barco.com/en/support/knowledge-base/KB12686	A-BAR-CONT-200622/45
Vendor: BD					
Product: synapsys					
Insufficient Session Expiration	02-Jun-22	5.7	BD Synapsys™, versions 4.20, 4.20 SR1, and 4.30,	https://cybersecurity.bd.com/bulletins-and-	A-BD-SYNA-200622/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain an insufficient session expiration vulnerability. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). **CVE ID : CVE-2022-30277**	patches/bd-synapsys-insufficient-session-expiration	
Vendor: bigbluebutton					
Product: bigbluebutton					
Improper Input Validation	01-Jun-22	7.5	BigBlueButton is an open source web conferencing system. Versions starting with 2.2 and prior to 2.3.19, 2.4.7, and 2.5.0-beta.2 are vulnerable to regular expression denial of service (ReDoS) attacks. By using specific a RegularExpression, an attacker can cause denial of service for the bbb-html5 service. The useragent library performs checking of device by parsing the input of User-Agent header and lets it go	https://github.com/bigbluebutton/bigbluebutton/pull/14896, https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-rwrv-p665-4vwp, https://github.com/bigbluebutton/bigbluebutton/pull/14886	A-BIG-BIGB-200622/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through lookupUserAgent() (alias of useragent.lookup()). This function handles input by regexing and attackers can abuse that by providing some ReDos payload using `SmartWatch`. The maintainers removed `htmlclient/useragent` from versions 2.3.19, 2.4.7, and 2.5.0-beta.2. As a workaround, disable NginX forwarding the requests to the handler according to the directions in the GitHub Security Advisory. **CVE ID : CVE-2022-29169**		
Exposure of Sensitive Information to an Unauthorized Actor	01-Jun-22	6.5	BigBlueButton is an open source web conferencing system. Starting with version 2.2 and prior to versions 2.3.9 and 2.4-beta-1, an attacker can circumvent access controls to obtain the content of public chat messages from different meetings on the server. The attacker must be a participant in a meeting on the server.	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-3fqh-p4qr-vfm9, https://github.com/bigbluebutton/bigbluebutton/pull/12861	A-BIG-BIGB-200622/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BigBlueButton versions 2.3.9 and 2.4-beta-1 contain a patch for this issue. There are currently no known workarounds. **CVE ID : CVE-2022-29232**		
Improper Authorization	02-Jun-22	4.3	BigBlueButton is an open source web conferencing system. In BigBlueButton starting with 2.2 but before 2.3.18 and 2.4-rc-1, an attacker can circumvent access controls to gain access to all breakout rooms of the meeting they are in. The permission checks rely on knowledge of internal ids rather than on verification of the role of the user. Versions 2.3.18 and 2.4-rc-1 contain a patch for this issue. There are currently no known workarounds. **CVE ID : CVE-2022-29233**	https://github.com/bigbluebutton/bigbluebutton/pull/14265, https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-3mr9-p9gw-cf33, https://github.com/bigbluebutton/bigbluebutton/pull/13117	A-BIG-BIGB-200622/49
Improper Authorization	02-Jun-22	4.3	BigBlueButton is an open source web conferencing system. Starting in version 2.2 and up to versions 2.3.18 and 2.4.1, an attacker could send messages	https://github.com/bigbluebutton/bigbluebutton/pull/13850, https://github.com/bigbluebutton/bigbluebutton/pull/14265,	A-BIG-BIGB-200622/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a locked chat within a grace period of 5s after the lock setting was enacted. The attacker needs to be a participant in the meeting. Versions 2.3.18 and 2.4.1 contain a patch for this issue. There are currently no known workarounds. **CVE ID : CVE-2022-29234**	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-36vc-c338-6xjv	
Exposure of Sensitive Information to an Unauthorized Actor	02-Jun-22	5.3	BigBlueButton is an open source web conferencing system. Starting in version 2.2 and up to versions 2.3.18 and 2.4-rc-6, an attacker who is able to obtain the meeting identifier for a meeting on a server can find information related to an external video being shared, like the current timestamp and play/pause. The problem has been patched in versions 2.3.18 and 2.4-rc-6 by modifying the stream to send the data only for users in the meeting. There are currently no known workarounds. **CVE ID : CVE-2022-29235**	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-x82p-j22f-v4q6, https://github.com/bigbluebutton/bigbluebutton/pull/14265, https://github.com/bigbluebutton/bigbluebutton/pull/13788	A-BIG-BIGB-200622/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	02-Jun-22	4.3	BigBlueButton is an open source web conferencing system. Starting in version 2.2 and up to versions 2.3.18 and 2.4-rc-6, an attacker can circumvent access restrictions for drawing on the whiteboard. The permission check is inadvertently skipped on the server, due to a previously introduced grace period. The attacker must be a meeting participant. The problem has been patched in versions 2.3.18 and 2.4-rc-6. There are currently no known workarounds. **CVE ID : CVE-2022-29236**	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-p93g-r9gm-9v6r, https://github.com/bigbluebutton/bigbluebutton/pull/14265, https://github.com/bigbluebutton/bigbluebutton/pull/13803	A-BIG-BIGB-200622/52
Product: greenlight					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	BigBlueButton Greenlight 2.11.1 allows XSS. A threat actor could have a username containing a JavaScript payload. The payload gets executed in the browser of the victim in the "Share room access" dialog if the victim has shared access to the particular room with	https://www.mgm-sp.com/en/cve-2022-26497-bigbluebutton-greenlight-xss/	A-BIG-GREE-200622/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker previously. **CVE ID : CVE-2022-26497**		
Vendor: blackrainbow					
Product: nimbus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	Black Rainbow NIMBUS before 3.7.0 allows stored Cross-site Scripting (XSS). **CVE ID : CVE-2022-24967**	https://blackrainbow.com/corporate/	A-BLA-NIMB-200622/54
Vendor: Bonitasoft					
Product: bonita_web					
Incorrect Authorization	02-Jun-22	9.8	Bonita Web 2021.2 is affected by a authentication/authorization bypass vulnerability due to an overly broad exclude pattern used in the RestAPIAuthorizationFilter. By appending ;i18ntranslation or /../i18ntranslation/ to the end of a URL, users with no privileges can access privileged API endpoints. This can lead to remote code execution by abusing the privileged API actions. **CVE ID : CVE-2022-25237**	N/A	A-BON-BONI-200622/55
Vendor: Bottlepy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bottle					
Improper Handling of Exceptional Conditions	02-Jun-22	9.8	Bottle before 0.12.20 mishandles errors during early request binding. **CVE ID : CVE-2022-31799**	https://github.com/bottlepy/bottle/commit/e140e1b54da721a660f2eb9d58a106b7b3ff2f00, https://github.com/bottlepy/bottle/commit/a2b0ee6bb4ce88895429ec4aca856616244c4c4c	A-BOT-BOTT-200622/56
Vendor: browsbox					
Product: brows_box					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	BrowsBox CMS v4.0 was discovered to contain a SQL injection vulnerability. **CVE ID : CVE-2022-29704**	N/A	A-BRO-BROW-200622/57
Vendor: caddyserver					
Product: caddy					
URL Redirection to Untrusted Site ('Open Redirect')	02-Jun-22	6.1	Caddy v2.4 was discovered to contain an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect users to arbitrary web URLs by tricking the victim users to click on crafted links.	https://github.com/caddyserver/caddy/pull/4499	A-CAD-CADD-200622/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29718		
Vendor: car_rental_management_system_project					
Product: car_rental_management_system					
Unrestricted Upload of File with Dangerous Type	02-Jun-22	9.8	Car Rental Management System v1.0 is vulnerable to Arbitrary code execution via car-rental-management-system/admin/ajax.php?action=save_car. **CVE ID : CVE-2022-32019**	N/A	A-CAR-CAR_-200622/59
N/A	02-Jun-22	9.8	Car Rental Management System v1.0 is vulnerable to Arbitrary code execution via ip/car-rental-management-system/admin/ajax.php?action=save_settings. **CVE ID : CVE-2022-32020**	N/A	A-CAR-CAR_-200622/60
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/manage_movement.php?id=. **CVE ID : CVE-2022-32021**	N/A	A-CAR-CAR_-200622/61
Improper Neutralization of Special Elements	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via /ip/car-rental-	N/A	A-CAR-CAR_-200622/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			management-system/admin/ajax.php?action=login. **CVE ID : CVE-2022-32022**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via car-rental-management-system/booking.php?car_id=. **CVE ID : CVE-2022-32024**	N/A	A-CAR-CAR_-200622/63
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/view_car.php?id=. **CVE ID : CVE-2022-32025**	N/A	A-CAR-CAR_-200622/64
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/manage_booking.php?id=. **CVE ID : CVE-2022-32026**	N/A	A-CAR-CAR_-200622/65
Improper Neutralization of Special Elements used in an SQL	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/index	N/A	A-CAR-CAR_-200622/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			.php?page=manage_car&id=. **CVE ID : CVE-2022-32027**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/manage_user.php?id=. **CVE ID : CVE-2022-32028**	N/A	A-CAR-CAR_-200622/67
Vendor: chatbot_app_with_suggestion_project					
Product: chatbot_app_with_suggestion					
N/A	02-Jun-22	6.5	ChatBot App with Suggestion v1.0 is vulnerable to Delete any file via /simple_chat_bot/classes/Master.php?f=delete_img. **CVE ID : CVE-2022-31966**	N/A	A-CHA-CHAT-200622/68
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	ChatBot App with Suggestion v1.0 is vulnerable to SQL Injection via /simple_chat_bot/admin/?page=user/manage_user&id=. **CVE ID : CVE-2022-31969**	N/A	A-CHA-CHAT-200622/69
Improper Neutralization of Special Elements used in an	02-Jun-22	7.2	ChatBot App with Suggestion v1.0 is vulnerable to SQL Injection via /simple_chat_bot/admin/?page=response	N/A	A-CHA-CHAT-200622/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			s/manage_response &id=. **CVE ID : CVE-2022-31970**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	ChatBot App with Suggestion v1.0 is vulnerable to SQL Injection via /simple_chat_bot/admin/?page=responses/view_response&id=. **CVE ID : CVE-2022-31971**	N/A	A-CHA-CHAT-200622/71
Vendor: churchcrm					
Product: churchcrm					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jun-22	7.2	There is a SQL Injection vulnerability in ChurchCRM 4.4.5 via the 'PersonID' field in /churchcrm/WhyCameEditor.php. **CVE ID : CVE-2022-31325**	N/A	A-CHU-CHUR-200622/72
Vendor: complete_online_job_search_system_project					
Product: complete_online_job_search_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/company/index.php?view=edit&id=. **CVE ID : CVE-2022-32007**	N/A	A-COM-COMP-200622/73
Improper Neutralizat	02-Jun-22	7.2	Complete Online Job Search System v1.0 is	N/A	A-COM-COMP-200622/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			vulnerable to SQL Injection via eris/admin/vacancy/index.php?view=edit&id=. **CVE ID : CVE-2022-32008**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/user/index.php?view=edit&id=. **CVE ID : CVE-2022-32010**	N/A	A-COM-COMP-200622/75
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/applicants/index.php?view=view&id=. **CVE ID : CVE-2022-32011**	N/A	A-COM-COMP-200622/76
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/employee/index.php?view=edit&id=. **CVE ID : CVE-2022-32012**	N/A	A-COM-COMP-200622/77
Improper Neutralization of Special Elements	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via eris/admin/category	N/A	A-COM-COMP-200622/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			/index.php?view=edit&id=. **CVE ID : CVE-2022-32013**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=result&searchfor=byfunction. **CVE ID : CVE-2022-32014**	N/A	A-COM-COMP-200622/79
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=category&search=. **CVE ID : CVE-2022-32015**	N/A	A-COM-COMP-200622/80
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=result&searchfor=bycompany. **CVE ID : CVE-2022-32016**	N/A	A-COM-COMP-200622/81
Improper Neutralization of Special Elements used in an SQL Command	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=result&searchfor=bytitle.	N/A	A-COM-COMP-200622/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-32017**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=hiring&search=. **CVE ID : CVE-2022-32018**	N/A	A-COM-COMP-200622/83
Vendor: couchbase					
Product: bleve					
Missing Authentication for Critical Function	01-Jun-22	5.5	Bleve is a text indexing library for go. Bleve includes HTTP utilities under bleve/http package, that are used by its sample application. These HTTP methods pave way for exploitation of a node's filesystem where the bleve index resides, if the user has used bleve's own HTTP (bleve/http) handlers for exposing the access to the indexes. For instance, the CreateIndexHandler (`http/index_create.go`) and DeleteIndexHandler (`http/index_delete.go`) enable an attacker to create a bleve index (directory structure)	https://github.com/blevesearch/bleve/security/advisories/GHSA-9w9f-6mg8-jp7w, https://github.com/blevesearch/bleve/commit/1c7509d6a17d36f265c90b4e8f4e3a3182fe79ff	A-COU-BLEV-200622/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			anywhere where the user running the server has the write permissions and to delete recursively any directory owned by the same user account. Users who have used the bleve/http package for exposing access to bleve index without the explicit handling for the Role Based Access Controls(RBAC) of the index assets would be impacted by this issue. There is no patch for this issue because the http package is purely intended to be used for demonstration purposes. Bleve was never designed handle the RBACs, nor it was ever advertised to be used in that way. The collaborators of this project have decided to stay away from adding any authentication or authorization to bleve project at the moment. The bleve/http package is mainly for demonstration purposes and it lacks exhaustive validation		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the user inputs as well as any authentication and authorization measures. It is recommended to not use bleve/http in production use cases. **CVE ID : CVE-2022-31022**		
Vendor: creatiwity					
Product: witycms					
Unrestricted Upload of File with Dangerous Type	02-Jun-22	8.8	An arbitrary file upload in the image upload component of wityCMS v0.6.2 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-29725**	N/A	A-CRE-WITY-200622/85
Vendor: Dell					
Product: powerscale_onefs					
Weak Password Requirements	01-Jun-22	7.5	Dell PowerScale OneFS versions 8.2.0.x through 9.3.0.x, contain a weak password requirement vulnerability. An administrator may create an account with no password. A remote attacker may potentially exploit this leading to a user account compromise. **CVE ID : CVE-2022-29098**	https://www.dell.com/support/kbdoc/en-us/000200128/dsa-2022-082-dell-emc-powerscale-onefs-security-update?lang=en	A-DEL-POWE-200622/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: unityvsa_operating_environment					
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	Dell Unity, Dell UnityVSA, and Dell Unity XT versions before 5.2.0.0.5.173 do not restrict excessive authentication attempts in Unisphere GUI. A remote unauthenticated attacker may potentially exploit this vulnerability to brute-force passwords and gain access to the system as the victim. Account takeover is possible if weak passwords are used by users. **CVE ID : CVE-2022-29084**	https://www.dell.com/support/kbdoc/000199050	A-DEL-UNIT-200622/87
Insufficiently Protected Credentials	02-Jun-22	6.7	Dell Unity, Dell UnityVSA, and Dell Unity XT versions prior to 5.2.0.0.5.173 contain a plain-text password storage vulnerability when certain off-array tools are run on the system. The credentials of a user with high privileges are stored in plain text. A local malicious user with high privileges may use the exposed password to gain	https://www.dell.com/support/kbdoc/000199050	A-DEL-UNIT-200622/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access with the privileges of the compromised user. **CVE ID : CVE-2022-29085**		
Product: unity_operating_environment					
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	Dell Unity, Dell UnityVSA, and Dell Unity XT versions before 5.2.0.0.5.173 do not restrict excessive authentication attempts in Unisphere GUI. A remote unauthenticated attacker may potentially exploit this vulnerability to brute-force passwords and gain access to the system as the victim. Account takeover is possible if weak passwords are used by users. **CVE ID : CVE-2022-29084**	https://www.dell.com/support/kbdoc/000199050	A-DEL-UNIT-200622/89
Insufficiently Protected Credentials	02-Jun-22	6.7	Dell Unity, Dell UnityVSA, and Dell Unity XT versions prior to 5.2.0.0.5.173 contain a plain-text password storage vulnerability when certain off-array tools are run on the system. The credentials of a user with high privileges	https://www.dell.com/support/kbdoc/000199050	A-DEL-UNIT-200622/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are stored in plain text. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2022-29085**		
Product: unity_xt_operating_environment					
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	Dell Unity, Dell UnityVSA, and Dell Unity XT versions before 5.2.0.0.5.173 do not restrict excessive authentication attempts in Unisphere GUI. A remote unauthenticated attacker may potentially exploit this vulnerability to brute-force passwords and gain access to the system as the victim. Account takeover is possible if weak passwords are used by users. **CVE ID : CVE-2022-29084**	https://www.dell.com/support/kbdoc/000199050	A-DEL-UNIT-200622/91
Insufficiently Protected Credentials	02-Jun-22	6.7	Dell Unity, Dell UnityVSA, and Dell Unity XT versions prior to 5.2.0.0.5.173 contain a plain-text password storage	https://www.dell.com/support/kbdoc/000199050	A-DEL-UNIT-200622/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when certain off-array tools are run on the system. The credentials of a user with high privileges are stored in plain text. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2022-29085**		
Vendor: devcert_project					
Product: devcert					
Incorrect Comparison	02-Jun-22	7.5	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the devcert npm package, when an attacker is able to supply arbitrary input to the certificateFor method **CVE ID : CVE-2022-1929**	N/A	A-DEV-DEVC-200622/93
Vendor: dhis2					
Product: dhis_2					
Improper Neutralization of Special Elements used in an	01-Jun-22	8.8	DHIS2 is an information system for data capture, management, validation, analytics and visualization. A	https://github.com/dhis2/dhis2-core/pull/10953, https://github.c	A-DHI-DHIS-200622/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			SQL injection security vulnerability affects the `/api/programs/orgUnits?programs=` API endpoint in DHIS2 versions prior to 2.36.10.1 and 2.37.6.1. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. The vulnerability is not exposed to a non-malicious user and requires a conscious attack to be exploited. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance's database. Security patches are now available for DHIS2 versions 2.36.10.1 and 2.37.6.1. One may apply mitigations at the web proxy level as a workaround. More information about these mitigations is available in the	om/dhis2/dhis2-core/commit/ef04483a9b177d62e48dcf4e498b302a11f95e7d, https://github.com/dhis2/dhis2-core/commit/3b245d04a58b78f0dc9bae8559f36ee4ca36dfac	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GitHub Security Advisory. **CVE ID : CVE-2022-24848**		
Vendor: discourse					
Product: discourse					
Incorrect Authorization	07-Jun-22	5.3	Discourse is an open source platform for community discussion. Prior to version 2.8.4 on the `stable` branch and 2.9.0beta5 on the `beta` and `tests-passed` branches, inviting users on sites that use single sign-on could bypass the `must_approve_users` check and invites by staff are always approved automatically. The issue is patched in Discourse version 2.8.4 on the `stable` branch and version `2.9.0.beta5` on the `beta` and `tests-passed` branches. As a workaround, disable invites or increase `min_trust_level_to_allow_invite` to reduce the attack surface to more trusted users. **CVE ID : CVE-2022-31025**	https://github.com/discourse/discourse/security/advisories/GHSA-x7jh-mx5q-6f9q, https://github.com/discourse/discourse/commit/7c4e2d33fa4b922354c177ffc880a2f2701a91f9, https://github.com/discourse/discourse/commit/0fa0094531efc82d9371f90a02aa804b176d59cf	A-DIS-DISC-200622/95
Vendor: Dolibarr					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dolibarr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-22	6.1	Dolibarr 12.0.5 is vulnerable to Cross Site Scripting (XSS) via Sql Error Page. **CVE ID : CVE-2022-30875**	N/A	A-DOL-DOLI-200622/96
Vendor: Drupal					
Product: saml_sp_2.0_single_sign_on					
Improper Certificate Validation	03-Jun-22	8.8	Multiple vulnerabilities vulnerability in Drupal SAML SP 2.0 Single Sign On (SSO) - SAML Service Provider in certain non-default configurations allow a malicious user to login as any chosen user. The vulnerability is mitigated by the module's default settings which require the options "Either sign SAML assertions" and "x509 certificate". This issue affects: Drupal SAML SP 2.0 Single Sign On (SSO) - SAML Service Provider 8.x version 8.x-2.24 and prior versions; 7.x version 7.x-2.57 and prior versions.	https://www.drupal.org/sa-contrib-2021-036	A-DRU-SAML-200622/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26493		
Vendor: ecommerce-project-with-php-and-mysqli-fruits-bazar_project					
Product: ecommerce-project-with-php-and-mysqli-fruits-bazar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Ecommerce-project-with-php-and-mysqli-Fruits-Bazar 1.0 is vulnerable to SQL Injection in \search_product.php via the keyword parameters. **CVE ID : CVE-2022-30478**	N/A	A-ECO-ECOM-200622/98
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	4.8	Ecommerce-project-with-php-and-mysqli-Fruits-Bazar-1.0 is vulnerable to Cross Site Scripting (XSS) in \admin\add_cata.php via the ctg_name parameters. **CVE ID : CVE-2022-30482**	N/A	A-ECO-ECOM-200622/99
Vendor: eginnovations					
Product: eg_agent					
Improper Preservation of Permissions	02-Jun-22	7.8	eG Agent before 7.2 has weak file permissions that enable escalation of privileges to SYSTEM. **CVE ID : CVE-2022-29594**	N/A	A-EGI-EG_A-200622/100
Product: eg_manager					
Improper Preservation of	02-Jun-22	7.8	eG Agent before 7.2 has weak file permissions that enable escalation of	N/A	A-EGI-EG_M-200622/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			privileges to SYSTEM. **CVE ID : CVE-2022-29594**		
Product: eg_rum_collectors					
Improper Preservation of Permissions	02-Jun-22	7.8	eG Agent before 7.2 has weak file permissions that enable escalation of privileges to SYSTEM. **CVE ID : CVE-2022-29594**	N/A	A-EGI-EG_R-200622/102
Product: vm_agent					
Improper Preservation of Permissions	02-Jun-22	7.8	eG Agent before 7.2 has weak file permissions that enable escalation of privileges to SYSTEM. **CVE ID : CVE-2022-29594**	N/A	A-EGI-VM_A-200622/103
Vendor: Elastic					
Product: elasticsearch					
N/A	06-Jun-22	7.5	A Denial of Service flaw was discovered in Elasticsearch. Using this vulnerability, an unauthenticated attacker could forcibly shut down an Elasticsearch node with a specifically formatted network request. **CVE ID : CVE-2022-23712**	https://www.elastic.co/community/security/, https://discuss.elastic.co/t/elastic-stack-7-17-4-and-8-2-1-security-update/305530	A-ELA-ELAS-200622/104
Vendor: Elitecms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: elite_cms					
Improper Privilege Management	02-Jun-22	6.5	elitecms v1.01 is vulnerable to Delete any file via /admin/delete_image.php?file=. **CVE ID : CVE-2022-30804**	N/A	A-ELI-ELIT-200622/105
Unrestricted Upload of File with Dangerous Type	02-Jun-22	9.8	elitecms 1.0.1 is vulnerable to Arbitrary code execution via admin/manage_uploads.php. **CVE ID : CVE-2022-30808**	N/A	A-ELI-ELIT-200622/106
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	elitecms 1.01 is vulnerable to SQL Injection via /admin/edit_page.php?page=. **CVE ID : CVE-2022-30809**	N/A	A-ELI-ELIT-200622/107
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	elitecms v1.01 is vulnerable to SQL Injection via admin/edit_post.php. **CVE ID : CVE-2022-30810**	N/A	A-ELI-ELIT-200622/108
Improper Neutralization of Special Elements used in an	02-Jun-22	9.8	elitecms 1.01 is vulnerable to SQL Injection via /admin/add_post.php.	N/A	A-ELI-ELIT-200622/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			**CVE ID : CVE-2022-30813**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	elitecms v1.01 is vulnerable to SQL Injection via /admin/add_sidebar.php. **CVE ID : CVE-2022-30814**	N/A	A-ELI-ELIT-200622/110
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	elitecms 1.01 is vulnerable to SQL Injection via admin/edit_sidebar.php?page=2&sidebar= **CVE ID : CVE-2022-30815**	N/A	A-ELI-ELIT-200622/111
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	elitecms 1.01 is vulnerable to SQL Injection via /admin/edit_sidebar.php. **CVE ID : CVE-2022-30816**	N/A	A-ELI-ELIT-200622/112
Vendor: facturascripts					
Product: facturascripts					
Improper Neutralization of Input During Web Page	03-Jun-22	6.1	Cross-site Scripting (XSS) - Generic in GitHub repository neorazorx/facturascripts prior to 2022.09.	https://github.com/neorazorx/facturascripts/commit/93fc65ced3847a8e0837561e9fdfa0dbac	A-FAC-FACT-200622/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-1988**	e2cfcb, https://huntr.dev/bounties/7882a35a-b27e-4d7e-9fcc-e9e009d0b01c	
Vendor: fast_food_ordering_system_project					
Product: fast_food_ordering_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-22	4.8	A vulnerability classified as problematic has been found in Fast Food Ordering System 1.0. Affected is the file Master.php of the Master List. The manipulation of the argument Description with the input foo "><img src="" onerror="alert(document.cookie)"> leads to cross site scripting. It is possible to launch the attack remotely but it requires authentication. Exploit details have been disclosed to the public. **CVE ID : CVE-2022-1991**	N/A	A-FAS-FAST-200622/114
Vendor: flower_project					
Product: flower					
Improper Authentication	02-Jun-22	8.6	Flower, a web UI for the Celery Python RPC framework, all versions as of 05-02-2022 is vulnerable to an OAuth	N/A	A-FLO-FLOW-200622/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication bypass. An attacker could then access the Flower API to discover and invoke arbitrary Celery RPC calls or deny service by shutting down Celery task nodes. **CVE ID : CVE-2022-30034**		
Vendor: food-order-and-table-reservation-system_project					
Product: food-order-and-table-reservation-system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Food-order-and-table-reservation-system- 1.0 is vulnerable to SQL Injection in categorywise-menu.php via the catid parameters. **CVE ID : CVE-2022-30481**	N/A	A-FOO-FOOD-200622/116
Vendor: Freedesktop					
Product: freetype_demo_programs					
Out-of-bounds Write	02-Jun-22	7.8	ftbench.c in FreeType Demo Programs through 2.12.1 has a heap-based buffer overflow. **CVE ID : CVE-2022-31782**	N/A	A-FRE-FREE-200622/117
Product: libinput					
Use of Externally-Controlled Format String	02-Jun-22	7.8	A format string vulnerability was found in libinput **CVE ID : CVE-2022-1215**	N/A	A-FRE-LIBI-200622/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: friendsofflarum					
Product: upload					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	FriendsofFlarum (FoF) Upload is an extension that handles file uploads intelligently for your forum. If FoF Upload prior to version 1.2.3 is configured to allow the uploading of SVG files ('image/svg+xml'), navigating directly to an SVG file URI could execute arbitrary Javascript code decided by an attacker. This Javascript code could include the execution of HTTP web requests to Flarum, or any other web service. This could allow data to be leaked by an authenticated Flarum user, or, possibly, for data to be modified maliciously. This issue has been patched with v1.2.3, which now sanitizes uploaded SVG files. As a workaround, remove the ability for users to upload SVG files through FoF Upload. **CVE ID : CVE-2022-30999**	https://github.com/FriendsOfFlarum/upload/releases/tag/1.2.3, https://github.com/FriendsOfFlarum/upload/pull/318, https://github.com/FriendsOfFlarum/upload/security/advisories/GHSA-fm53-mpmp-7qw2	A-FRI-UPLO-200622/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: fudforum					
Product: fudforum					
Unrestricted Upload of File with Dangerous Type	06-Jun-22	7.2	FUDforum 3.1.2 is vulnerable to Remote Code Execution through Upload File feature of File Administration System in Admin Control Panel. **CVE ID : CVE-2022-30860**	N/A	A-FUD-FUDF-200622/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	4.8	FUDforum 3.1.2 is vulnerable to Stored XSS via Forum Name field in Forum Manager Feature. **CVE ID : CVE-2022-30861**	N/A	A-FUD-FUDF-200622/121
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	4.8	FUDForum 3.1.2 is vulnerable to Cross Site Scripting (XSS) via page_title param in Page Manager in the Admin Control Panel. **CVE ID : CVE-2022-30863**	N/A	A-FUD-FUDF-200622/122
Vendor: Gitlab					
Product: gitlab					
Uncontrolled Resource Consumption	06-Jun-22	2.7	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.3 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1783.json	A-GIT-GITL-200622/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 15.0 before 15.0.1. It may be possible for malicious group maintainers to add new members to a project within their group, through the REST API, even after their group owner enabled a setting to prevent members from being added to projects within that group. **CVE ID : CVE-2022-1783**		
Uncontrolled Resource Consumption	06-Jun-22	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.8 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. It may be possible for a subgroup member to access the members list of their parent group. **CVE ID : CVE-2022-1821**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1821.json	A-GIT-GITL-200622/124
Incorrect Authorization	06-Jun-22	6.5	Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1935.json	A-GIT-GITL-200622/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Trigger Token to misuse it from any location even when IP address restrictions were configured **CVE ID : CVE-2022-1935**		
Incorrect Authorization	06-Jun-22	6.5	Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Deploy Token to misuse it from any location even when IP address restrictions were configured **CVE ID : CVE-2022-1936**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1936.json	A-GIT-GITL-200622/126
Improper Neutralization of Input During Web Page Generation	06-Jun-22	5.4	A Stored Cross-Site Scripting vulnerability in Jira integration in GitLab EE affecting all versions from 13.11 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1940.json	A-GIT-GITL-200622/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf via specially crafted Jira Issues **CVE ID : CVE-2022-1940**		
Incorrect Authorization	06-Jun-22	7.1	When the feature is configured, improper authorization in the Interactive Web Terminal in GitLab CE/EE affecting all versions from 11.3 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1 allows users with the Developer role to open terminals on other Developers' running jobs **CVE ID : CVE-2022-1944**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1944.json	A-GIT-GITL-200622/128
Vendor: gogs					
Product: gogs					
Server-Side Request Forgery (SSRF)	01-Jun-22	6.5	Server-Side Request Forgery (SSRF) in GitHub repository gogs/gogs prior to 0.12.8. **CVE ID : CVE-2022-1285**	https://github.com/gogs/gogs/commit/7885f454a4946c4bbec1b4f8c603b5eea7429c7f, https://huntr.dev/bounties/da1fbd6e-7a02-458e-9c2e-6d226c47046d	A-GOG-GOGS-200622/129
Vendor: Gradle					
Product: gradle					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-22	7.2	Gradle Enterprise through 2022.2.2 has Incorrect Access Control that leads to code execution. **CVE ID : CVE-2022-30586**	https://security.gradle.com/advisory/2022-09, https://security.gradle.com	A-GRA-GRAD-200622/130
Product: gradle_enterprise					
Incorrect Authorization	06-Jun-22	7.5	Gradle Enterprise through 2022.2.2 has Incorrect Access Control that leads to information disclosure. **CVE ID : CVE-2022-30587**	https://security.gradle.com/advisory/2022-10, https://security.gradle.com	A-GRA-GRAD-200622/131
Vendor: grafana					
Product: grafana					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-22	7.5	Grafana 8.4.3 allows reading files via (for example) a /dashboard/snapshot/%7B%7Bconstructor.constructor'/../../../../../../../../etc/passwd URI. **CVE ID : CVE-2022-32275**	https://grafana.com	A-GRA-GRAF-200622/132
Vendor: hashicorp					
Product: nomad					
N/A	02-Jun-22	9.8	HashiCorp Nomad and Nomad Enterprise version 0.2.0 up to 1.3.0 were impacted by go-getter vulnerabilities enabling privilege escalation through the artifact stanza in submitted jobs onto	https://discuss.hashicorp.com/t/hcsec-2022-14-nomad-impacted-by-go-getter-vulnerabilities/39932, https://discuss.hashicorp.com	A-HAS-NOMA-200622/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the client agent host. Fixed in 1.1.14, 1.2.8, and 1.3.1. **CVE ID : CVE-2022-30324**		
Vendor: Haxx					
Product: curl					
Insufficiently Protected Credentials	02-Jun-22	5.7	An insufficiently protected credentials vulnerability exists in curl 4.9 to and include curl 7.82.0 are affected that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers. **CVE ID : CVE-2022-27774**	https://security.netapp.com/advisory/ntap-20220609-0008/	A-HAX-CURL-200622/134
N/A	02-Jun-22	7.5	An information disclosure vulnerability exists in curl 7.65.0 to 7.82.0 are vulnerable that by using an IPv6 address that was in the connection pool but with a different zone id it could reuse a connection instead. **CVE ID : CVE-2022-27775**	https://security.netapp.com/advisory/ntap-20220609-0008/	A-HAX-CURL-200622/135
Insufficiently	02-Jun-22	6.5	A insufficiently protected credentials	https://security.netapp.com/ad	A-HAX-CURL-200622/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			vulnerability in fixed in curl 7.83.0 might leak authentication or cookie header data on HTTP redirects to the same host but another port number. **CVE ID : CVE-2022-27776**	visory/ntap-20220609-0008/	
Use of Incorrectly-Resolved Name or Reference	02-Jun-22	8.1	A use of incorrectly resolved name vulnerability fixed in 7.83.1 might remove the wrong file when `--no-clobber` is used together with `--remove-on-error`. **CVE ID : CVE-2022-27778**	https://security.netapp.com/advisory/ntap-20220609-0009/	A-HAX-CURL-200622/137
Exposure of Resource to Wrong Sphere	02-Jun-22	5.3	libcurl wrongly allows cookies to be set for Top Level Domains (TLDs) if thehost name is provided with a trailing dot.curl can be told to receive and send cookies. curl's "cookie engine" can bebuilt with or without [Public Suffix List](https://publicsuffix.org/)awareness. If PSL support not provided, a more rudimentary check exists to atleast prevent cookies from being set on TLDs. This check was broken if thehost	https://security.netapp.com/advisory/ntap-20220609-0009/	A-HAX-CURL-200622/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name in the URL uses a trailing dot.This can allow arbitrary sites to set cookies that then would get sent to adifferent and unrelated site or domain. **CVE ID : CVE-2022-27779**		
Server-Side Request Forgery (SSRF)	02-Jun-22	7.5	The curl URL parser wrongly accepts percent-encoded URL separators like '/'when decoding the host name part of a URL, making it a *different* URL usingthe wrong host name when it is later retrieved.For example, a URL like `http://example.com%2F127.0.0.1/`, would be allowed bythe parser and get transposed into `http://example.com/127.0.0.1/`. This flawcan be used to circumvent filters, checks and more. **CVE ID : CVE-2022-27780**	https://security.netapp.com/advisory/ntap-20220609-0009/	A-HAX-CURL-200622/139
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jun-22	7.5	libcurl provides the `CURLOPT_CERTINFO` option to allow applications torequest details to be returned about a server's certificate chain.Due to an erroneous function, a	https://security.netapp.com/advisory/ntap-20220609-0009/	A-HAX-CURL-200622/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation. **CVE ID : CVE-2022-27781**		
Improper Certificate Validation	02-Jun-22	7.5	libcurl would reuse a previously created connection even when a TLS or SSHrelated option had been changed that should have prohibited reuse.libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse if one of them matches the setup. However, several TLS andSSH settings were left out from the configuration match checks, making themmatch too easily. **CVE ID : CVE-2022-27782**	https://security.netapp.com/advisory/ntap-20220609-0009/	A-HAX-CURL-200622/141
Cleartext Transmission of Sensitive Information	02-Jun-22	4.3	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP step even when HTTP is	https://security.netapp.com/advisory/ntap-20220609-0009/	A-HAX-CURL-200622/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided in theURL. This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when it built the HSTS cache. Or the otherway around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL. **CVE ID : CVE-2022-30115**		
Vendor: hornerautomation					
Product: cscape					
Out-of-bounds Write	02-Jun-22	7.8	The affected product is vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-27184**	N/A	A-HOR-CSCA-200622/143
Out-of-bounds Write	02-Jun-22	7.8	The affected product is vulnerable to an out-of-bounds write via uninitialized pointer, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-28690**	N/A	A-HOR-CSCA-200622/144
Out-of-bounds Read	02-Jun-22	7.8	The affected product is vulnerable to an out-of-bounds read via uninitialized	N/A	A-HOR-CSCA-200622/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-29488**		
Heap-based Buffer Overflow	02-Jun-22	7.8	The affected product is vulnerable to a heap-based buffer overflow via uninitialized pointer, which may allow an attacker to execute arbitrary code **CVE ID : CVE-2022-30540**	N/A	A-HOR-CSCA-200622/146
Vendor: IBM					
Product: infosphere_information_server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-22	9.8	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. **CVE ID : CVE-2022-31768**	https://www.ibm.com/support/pages/node/6592573, https://exchange.xforce.ibmcloud.com/vulnerabilities/227986	A-IBM-INFO-200622/147
Product: spectrum_protect_plus					
Insufficiently Protected Credentials	06-Jun-22	7.5	Credentials are printed in clear text in the IBM Spectrum Protect Plus 10.1.0.0 through 10.1.9.3 virgo log file in certain cases.	https://www.ibm.com/support/pages/node/6591505, https://exchange.xforce.ibmclou	A-IBM-SPEC-200622/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Credentials could be the remote vSnap, offload targets, or VADP credentials depending on the operation performed. Credentials that are using API key or certificate are not printed. IBM X-Force ID: 222231. **CVE ID : CVE-2022-22396**	d.com/vulnerabilities/222231	
Vendor: ict					
Product: protege_gx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	A cross-site scripting (XSS) vulnerability in ICT Protege GX/WX v2.08 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter. **CVE ID : CVE-2022-29734**	https://www.ict.co/	A-ICT-PROT-200622/149
Product: protege_wx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	A cross-site scripting (XSS) vulnerability in ICT Protege GX/WX v2.08 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter.	https://www.ict.co/	A-ICT-PROT-200622/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29734		
Vendor: Jamf					
Product: private_access					
Incorrect Authorization	07-Jun-22	7.5	Jamf Private Access before 2022-05-16 has Incorrect Access Control, in which an unauthorized user can reach a system in the internal infrastructure, aka WND-44801. **CVE ID : CVE-2022-29564**	https://jamf.com	A-JAM-PRIV-200622/151
Vendor: jflyfox					
Product: jfinal_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	A cross-site scripting (XSS) vulnerability in Jfinal CMS v5.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted X-Forwarded-For request. **CVE ID : CVE-2022-29648**	N/A	A-JFL-JFIN-200622/152
Vendor: jmespath_project					
Product: jmespath					
N/A	06-Jun-22	9.8	jmespath.rb (aka JMESPath for Ruby) before 1.6.1 uses JSON.load in a situation where JSON.parse is preferable. **CVE ID : CVE-2022-32511**	https://github.com/jmespath/jmespath.rb/pull/55	A-JME-JMES-200622/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: jodd					
Product: http					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Jun-22	7.5	Jodd HTTP v6.0.9 was discovered to contain multiple CLRF injection vulnerabilities via the components jodd.http.HttpRequest#set and `jodd.http.HttpRequest#send. These vulnerabilities allow attackers to execute Server-Side Request Forgery (SSRF) via a crafted TCP payload. **CVE ID : CVE-2022-29631**	N/A	A-JOD-HTTP-200622/154
Vendor: jpeg					
Product: libjpeg					
Out-of-bounds Read	02-Jun-22	6.5	libjpeg 1.63 has a heap-based buffer over-read in HierarchicalBitmapRequester::FetchRegion in hierarchicalbitmaprequester.cpp because the MCU size can be different between allocation and use. **CVE ID : CVE-2022-31796**	https://github.com/thorfdbg/libjpeg/commit/187035b9726710b4fe11d565c7808975c930895d	A-JPE-LIBJ-200622/155
Vendor: kitetech					
Product: keep_my_notes					
Improper Authentication	02-Jun-22	4.6	Keep My Notes v1.80.147 allows an attacker with physical access to the victim's device to	http://www.kitetech.co/keepmynotes	A-KIT-KEEP-200622/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the application's password/pin lock to access user data. This is possible due to lack of adequate security controls to prevent dynamic code manipulation. **CVE ID : CVE-2022-1716**		
Vendor: knime					
Product: analytics_platform					
Incorrect Default Permissions	02-Jun-22	7.8	In KNIME Analytics Platform below 4.6.0, the Windows installer sets improper filesystem permissions. **CVE ID : CVE-2022-31500**	https://www.knime.com/security/advisories#CVE-2022-31500, https://knime.com	A-KNI-ANAL-200622/157
Vendor: Kubernetes					
Product: cri-o					
Uncontrolled Resource Consumption	07-Jun-22	7.5	A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the Kube API. The ExecSync request runs commands in a container and logs the output of the command. This output is then read by CRI-O after command execution, and it is read in a manner where the	https://github.com/cri-o/cri-o/commit/f032cf649ecc7e0c46718bd9e7814bfb317cb544	A-KUB-CRI--200622/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entire file corresponding to the output of the command is read in. Thus, if the output of the command is large it is possible to exhaust the memory or the disk space of the node when CRI-O reads the output of the command. The highest threat from this vulnerability is system availability. **CVE ID : CVE-2022-1708**		
Vendor: Laravel					
Product: laravel					
Deserialization of Untrusted Data	07-Jun-22	9.8	Laravel 9.1.8, when processing attacker-controlled data for deserialization, allows Remote Code Execution (RCE) via an unserialized pop chain in __destruct in Illuminate\Broadcasting\PendingBroadcast.php and __call in Faker\Generator.php. **CVE ID : CVE-2022-31279**	N/A	A-LAR-LARA-200622/159
Vendor: libdwarf_project					
Product: libdwarf					
Out-of-bounds Read	02-Jun-22	7.8	libdwarf 0.4.0 has a heap-based buffer over-read in _dwarf_check_string_valid in dwarf_util.c.	https://github.com/davea42/libdwarf-code/commit/8151575a6ace77	A-LIB-LIBD-200622/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32200	d005ca5bb5d71c1bfdba3f7069	
Vendor: libjpeg_project					
Product: libjpeg					
NULL Pointer Dereference	02-Jun-22	5.5	In libjpeg 1.63, there is a NULL pointer dereference in Component::SubXOf in component.hpp. **CVE ID : CVE-2022-32201**	https://github.com/thorfdbg/libjpeg/commit/ea6315164b1649ff932a396b7600eac4bffcfaba	A-LIB-LIBJ-200622/161
NULL Pointer Dereference	02-Jun-22	5.5	In libjpeg 1.63, there is a NULL pointer dereference in LineBuffer::FetchRegion in linebuffer.cpp. **CVE ID : CVE-2022-32202**	https://github.com/thorfdbg/libjpeg/commit/51c3241b6da39df30f016b63f43f31c4011222c7	A-LIB-LIBJ-200622/162
Vendor: liblouis					
Product: liblouis					
Out-of-bounds Write	02-Jun-22	5.5	Liblouis 3.21.0 has an out-of-bounds write in compileRule in compileTranslationTable.c, as demonstrated by lou_trace. **CVE ID : CVE-2022-31783**	https://github.com/liblouis/liblouis/commit/ff747ec5e1ac54d54194846f6fe5bfc689192a85	A-LIB-LIBL-200622/163
Vendor: libmobi_project					
Product: libmobi					
Out-of-bounds Read	03-Jun-22	8.1	Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11. **CVE ID : CVE-2022-1987**	https://huntr.dev/bounties/e8197737-7557-443e-a59f-2a86e8dda75f, https://github.com/bfabiszews	A-LIB-LIBM-200622/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ki/libmobi/commit/612562bc1ea38f1708b044e7a079c47a05b1291d	
NULL Pointer Dereference	02-Jun-22	6.5	libmobi before v0.10 contains a NULL pointer dereference via the component mobi_buffer_getpointer. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted mobi file. **CVE ID : CVE-2022-29788**	https://github.com/bfabiszewski/libmobi/commit/ce0ab6586069791b1e8e2a42f44318e581c39939	A-LIB-LIBM-200622/165
Vendor: librehealth					
Product: librehealth_ehr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	6.1	Cross Site scripting (XSS) vulnerability inLibreHealth EHR Base 2.0.0 via interface/usergroup/usergroup_admin_add.php Username. **CVE ID : CVE-2022-31492**	N/A	A-LIB-LIBR-200622/166
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	6.1	LibreHealth EHR Base 2.0.0 allows gacl/admin/acl_admin.php acl_id XSS. **CVE ID : CVE-2022-31493**	N/A	A-LIB-LIBR-200622/167
Improper Neutralization of Input	06-Jun-22	6.1	LibreHealth EHR Base 2.0.0 allows gacl/admin/acl_admin.php action XSS.	N/A	A-LIB-LIBR-200622/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-31494**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-22	6.1	LibreHealth EHR Base 2.0.0 allows gacl/admin/acl_admin.php return_page XSS. **CVE ID : CVE-2022-31495**	N/A	A-LIB-LIBR-200622/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	6.1	LibreHealth EHR Base 2.0.0 allows interface/orders/patient_match_dialog.php key XSS. **CVE ID : CVE-2022-31498**	N/A	A-LIB-LIBR-200622/170
Vendor: librenms					
Product: librenms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	LibreNMS v22.3.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /Table/GraylogController.php. **CVE ID : CVE-2022-29711**	https://github.com/librenms/librenms/pull/13931, https://github.com/librenms/librenms/commit/cc6112b8fb36039b862b42d86eb79ef7ee89d31b	A-LIB-LIBR-200622/171
Improper Neutralization of Special Elements used in a	02-Jun-22	9.8	LibreNMS v22.3.0 was discovered to contain multiple command injection vulnerabilities via the service_ip,	https://github.com/librenms/librenms/pull/13932	A-LIB-LIBR-200622/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			hostname, and service_param parameters. **CVE ID : CVE-2022-29712**		
Vendor: lightbend					
Product: play_framework					
Uncontrolled Resource Consumption	02-Jun-22	7.5	Play Framework is a web framework for Java and Scala. A denial of service vulnerability has been discovered in verions 2.8.3 through 2.8.15 of Play's forms library, in both the Scala and Java APIs. This can occur when using either the `Form#bindFromRequest` method on a JSON request body or the `Form#bind` method directly on a JSON value. If the JSON data being bound to the form contains a deeply-nested JSON object or array, the form binding implementation may consume all available heap space and cause an `OutOfMemoryError`. If executing on the default dispatcher and `akka.jvm-exit-on-fatal-error` is enabled—as it is by default—then this can crash the	https://github.com/playframework/playframework/security/advisories/GHSA-v8x6-59g4-5g3w, https://github.com/playframework/playframework/pull/11301	A-LIG-PLAY-200622/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application process. `Form.bindFromRequest` is vulnerable when using any body parser that produces a type of `AnyContent` or `JsValue` in Scala, or one that can produce a `JsonNode` in Java. This includes Play's default body parser. This vulnerability been patched in version 2.8.16. There is now a global limit on the depth of a JSON object that can be parsed, which can be configured by the user if necessary. As a workaround, applications that do not need to parse a request body of type `application/json` can switch from the default body parser to another body parser that supports only the specific type of body they expect. **CVE ID : CVE-2022-31018**		
Generation of Error Message Containing Sensitive Information	02-Jun-22	7.5	Play Framework is a web framework for Java and Scala. Verions prior to 2.8.16 are vulnerable to generation of error messages containing sensitive information. Play	https://github.com/playframework/playframework/security/advisories/GHSA-p9p4-97g9-wcrh, https://github.com/playframew	A-LIG-PLAY-200622/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Framework, when run in dev mode, shows verbose errors for easy debugging, including an exception stack trace. Play does this by configuring its `DefaultHttpErrorHandler` to do so based on the application mode. In its Scala API Play also provides a static object `DefaultHttpErrorHandler` that is configured to always show verbose errors. This is used as a default value in some Play APIs, so it is possible to inadvertently use this version in production. It is also possible to improperly configure the `DefaultHttpErrorHandler` object instance as the injected error handler. Both of these situations could result in verbose errors displaying to users in a production application, which could expose sensitive information from the application. In particular, the constructor for	ork/playframework/pull/11305	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`CORSFilter` and `apply` method for `CORSActionBuilder` use the static object `DefaultHttpErrorHandler` as a default value. This is patched in Play Framework 2.8.16. The `DefaultHttpErrorHandler` object has been changed to use the prod-mode behavior, and `DevHttpErrorHandler` has been introduced for the dev-mode behavior. A workaround is available. When constructing a `CORSFilter` or `CORSActionBuilder`, ensure that a properly-configured error handler is passed. Generally this should be done by using the `HttpErrorHandler` instance provided through dependency injection or through Play's `BuiltInComponents`. Ensure that the application is not using the `DefaultHttpErrorHandler` static object in any code that may be run in production.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31023		
Vendor: linkplay					
Product: sound_bar					
Use of Hard-coded Credentials	02-Jun-22	9.8	LinkPlay Sound Bar v1.0 allows attackers to escalate privileges via a hardcoded password for the SSL certificate. **CVE ID : CVE-2022-28605**	N/A	A-LIN-SOUN-200622/175
Vendor: Linux					
Product: linux_kernel					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jun-22	6.3	An out-of-bounds read flaw was found in the Linux kernel's TeleTYpe subsystem. The issue occurs in how a user triggers a race condition using ioctls TIOCSPTLCK and TIOCGPTPEER and TIOCSTI and TCXONC with leakage of memory in the flush_to_ldisc function. This flaw allows a local user to crash the system or read unauthorized random data from memory. **CVE ID : CVE-2022-1462**	N/A	A-LIN-LINU-200622/176
Out-of-bounds Write	02-Jun-22	5.5	A flaw out of bounds memory write in the Linux kernel UDF file system functionality was found in the way user triggers some	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c1ad35dd05	A-LIN-LINU-200622/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file operation which triggers udf_write_fi(). A local user could use this flaw to crash the system or potentially **CVE ID : CVE-2022-1943**	48ce947d97aaf92f7f2f9a202951cf	
Insufficiently Protected Credentials	06-Jun-22	7.5	Credentials are printed in clear text in the IBM Spectrum Protect Plus 10.1.0.0 through 10.1.9.3 virgo log file in certain cases. Credentials could be the remote vSnap, offload targets, or VADP credentials depending on the operation performed. Credentials that are using API key or certificate are not printed. IBM X-Force ID: 222231. **CVE ID : CVE-2022-22396**	https://www.ibm.com/support/pages/node/6591505, https://exchange.xforce.ibmcloud.com/vulnerabilities/222231	A-LIN-LINU-200622/178
Vendor: mattermost					
Product: mattermost_server					
Uncontrolled Resource Consumption	02-Jun-22	6.5	Uncontrolled resource consumption in Mattermost version 6.6.0 and earlier allows an authenticated attacker to crash the server via a crafted SVG attachment on a post.	https://mattermost.com/security-updates/	A-MAT-MATT-200622/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1982		
Vendor: merchandise_online_store_project					
Product: merchandise_online_store					
Unrestricted Upload of File with Dangerous Type	02-Jun-22	9.8	Merchandise Online Store v1.0 by oretnom23 has an arbitrary code execution (RCE) vulnerability in the user profile upload point in the system information. **CVE ID : CVE-2022-30423**	N/A	A-MER-MERC-200622/180
Vendor: Microsoft					
Product: edge_chromium					
N/A	01-Jun-22	4.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability. **CVE ID : CVE-2022-26905**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26905	A-MIC-EDGE-200622/181
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Jun-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30128. **CVE ID : CVE-2022-30127**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30127	A-MIC-EDGE-200622/182
Concurrent Execution using Shared Resource with	01-Jun-22	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-EDGE-200622/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			from CVE-2022-30127. **CVE ID : CVE-2022-30128**	ory/CVE-2022-30128	
Vendor: mingsoft					
Product: mcms					
Cross-Site Request Forgery (CSRF)	02-Jun-22	8.8	An issue was discovered in MCMS 5.2.7. There is a CSRF vulnerability that can add an administrator account via ms/basic/manager/save.do. **CVE ID : CVE-2022-29647**	N/A	A-MIN-MCMS-200622/184
Unrestricted Upload of File with Dangerous Type	02-Jun-22	9.8	An arbitrary file upload vulnerability was discovered in MCMS 5.2.7, allowing an attacker to execute arbitrary code through a crafted ZIP file. **CVE ID : CVE-2022-30506**	N/A	A-MIN-MCMS-200622/185
Vendor: minio					
Product: minio					
Uncontrolled Resource Consumption	07-Jun-22	7.5	MinIO is a multi-cloud object storage solution. Starting with version RELEASE.2019-09-25T18-25-51Z and ending with version RELEASE.2022-06-02T02-11-04Z, MinIO is vulnerable to an unending go-routine buildup	https://github.com/minio/minio/security/advisories/GHSA-qrpr-r3pw-f636, https://github.com/minio/minio/pull/14995	A-MIN-MINI-200622/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while keeping connections established due to HTTP clients not closing the connections. Public-facing MinIO deployments are most affected. Users should upgrade to RELEASE.2022-06-02T02-11-04Z to receive a patch. One possible workaround is to use a reverse proxy to limit the number of connections being attempted in front of MinIO, and actively rejecting connections from such malicious clients. **CVE ID : CVE-2022-31028**		
Vendor: Mitre					
Product: cve-services					
Cleartext Storage of Sensitive Information	02-Jun-22	7.5	CVEProject/cve-services is an open source project used to operate the CVE services API. A conditional in 'data.js' has potential for production secrets to be written to disk. The affected method writes the generated randomKey to disk if the environment is not development. If this method were	https://github.com/CVEProject/cve-services/security/advisories/GHSA-mpwm-rmqp-7629	A-MIT-CVE--200622/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			called in production, it is possible that it would write the plaintext key to disk. A patch is not available as of time of publication but is anticipated as a "hot fix" for version 1.1.1 and for the 2.x branch. **CVE ID : CVE-2022-31004**		
Vendor: mv					
Product: idce					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.5	SQL injection in Logon Page of IDCE MV's application, version 1.0, allows an attacker to inject SQL payloads in the user field, connecting to a database to access enterprise's private and sensitive information. **CVE ID : CVE-2022-30496**	N/A	A-MV-IDCE-200622/188
Vendor: nebulab					
Product: solidus					
Cross-Site Request Forgery (CSRF)	01-Jun-22	4.3	solidus_backend is the admin interface for the Solidus e-commerce framework. Versions prior to 3.1.6, 3.0.6, and 2.11.16 contain a cross-site request forgery (CSRF) vulnerability. The vulnerability allows	https://github.com/solidusio/solidus/commit/de796a2e0be7f154cae48b46e267501559d9716c, https://github.com/solidusio/solidus/security/advisories/GH	A-NEB-SOLI-200622/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to change the state of an order's adjustments if they hold its number, and the execution happens on a store administrator's computer. Users should upgrade to solidus_backend 3.1.6, 3.0.6, or 2.11.16 to receive a patch. **CVE ID : CVE-2022-31000**	SA-8639-qx56-r428	
Vendor: neos					
Product: neos_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	Multiple cross-site scripting (XSS) vulnerabilities in Neos CMS allow attackers with the editor role or higher to inject arbitrary script or HTML code using the editor function, the deletion of assets, or a workspace title. The vulnerabilities were found in versions 3.3.29 and 8.0.1 and could also be present in all intermediate versions. **CVE ID : CVE-2022-30429**	https://www.neos.io/blog/xss-in-various-backend-modules.html	A-NEO-NEOS-200622/190
Vendor: Netapp					
Product: e-series_santricity_os_controller					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	02-Jun-22	4.4	E-Series SANtricity OS Controller Software versions 11.40 through 11.70.2 store the LDAP BIND password in plaintext within a file accessible only to privileged users. **CVE ID : CVE-2022-23236**	https://security.netapp.com/advisory/NTAP-20220527-0001/	A-NET-E-SE-200622/191
URL Redirection to Untrusted Site ('Open Redirect')	02-Jun-22	6.1	E-Series SANtricity OS Controller Software 11.x versions through 11.70.2 are vulnerable to host header injection attacks that could allow an attacker to redirect users to malicious websites. **CVE ID : CVE-2022-23237**	https://security.netapp.com/advisory/NTAP-20220527-0002/	A-NET-E-SE-200622/192
Product: solidfire\,_enterprise_sds_\&_hci_storage_node					
Cleartext Transmission of Sensitive Information	02-Jun-22	4.3	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP step even when HTTP is provided in theURL. This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when it built the HSTS cache.	https://security.netapp.com/advisory/ntap-20220609-0009/	A-NET-SOLI-200622/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Or the otherway around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL. **CVE ID : CVE-2022-30115**		
Vendor: Nextcloud					
Product: richdocuments					
Improper Access Control	02-Jun-22	6.5	richdocuments is the repository for NextCloud Collabra, the app for Nextcloud Office collaboration. Prior to versions 6.0.0, 5.0.4, and 4.2.6, a user could be tricked into working against a remote Office by sending them a federated share. richdocuments versions 6.0.0, 5.0.4 and 4.2.6 contain a fix for this issue. There are currently no known workarounds available. **CVE ID : CVE-2022-31024**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-94hr-7g4v-f53r, https://github.com/nextcloud/richdocuments/pull/2161	A-NEX-RICH-200622/194
Vendor: Nginx					
Product: njs					
N/A	02-Jun-22	5.5	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function	https://github.com/nginx/njs/commit/2e00e95473861846aa	A-NGI-NJS-200622/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			njs_value_own_enumerate at src/njs_value.c. **CVE ID : CVE-2022-29779**	8538be87db07699d9f676d	
N/A	02-Jun-22	5.5	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_array_prototype_sort at src/njs_array.c. **CVE ID : CVE-2022-29780**	https://github.com/nginx/njs/commit/8b39afdad9a0761e0a5d4af1a762bd9a6daef572	A-NGI-NJS-200622/196
N/A	02-Jun-22	5.5	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_set_number at src/njs_value.h. **CVE ID : CVE-2022-30503**	https://github.com/nginx/njs/commit/5c6130a2a0b4c41ab415f6b8992aa323636338b9	A-NGI-NJS-200622/197
Vendor: ofcms_project					
Product: ofcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	OFCMS v1.1.4 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/comn/service/update.json. **CVE ID : CVE-2022-29653**	N/A	A-OFC-OFCM-200622/198
Vendor: online_car_wash_booking_system_project					
Product: online_car_wash_booking_system					
N/A	02-Jun-22	6.5	Online Car Wash Booking System v1.0 is vulnerable to	N/A	A-ONL-ONLI-200622/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Delete any file via /ocwbs/classes/Master.php?f=delete_img. **CVE ID : CVE-2022-31342**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/?page=bookings/view_details&id=. **CVE ID : CVE-2022-31343**	N/A	A-ONL-ONLI-200622/200
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_booking. **CVE ID : CVE-2022-31344**	N/A	A-ONL-ONLI-200622/201
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/?page=user/manage_user&id=. **CVE ID : CVE-2022-31345**	N/A	A-ONL-ONLI-200622/202
Improper Neutralization of Special Elements used in an SQL	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_service.	N/A	A-ONL-ONLI-200622/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2022-31346**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_vehicle. **CVE ID : CVE-2022-31347**	N/A	A-ONL-ONLI-200622/204
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/bookings/update_status.php?id=. **CVE ID : CVE-2022-31348**	N/A	A-ONL-ONLI-200622/205
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/vehicles/manage_vehicle.php?id=. **CVE ID : CVE-2022-31350**	N/A	A-ONL-ONLI-200622/206
Improper Neutralization of Special Elements used in an SQL Command	02-Jun-22	9.8	Online Car Wash Booking System v1.0 by oretnom23 has SQL injection via /ocwbs/admin/services/manage_price.php?id=. **CVE ID : CVE-2022-31351**	N/A	A-ONL-ONLI-200622/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 by oretnom23 has SQL injection in /ocwbs/admin/services/manage_service.php?id=. **CVE ID : CVE-2022-31352**	N/A	A-ONL-ONLI-200622/208
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/services/view_service.php?id=. **CVE ID : CVE-2022-31353**	N/A	A-ONL-ONLI-200622/209
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=get_vehicle_service. **CVE ID : CVE-2022-31354**	N/A	A-ONL-ONLI-200622/210
Vendor: online_fire_reporting_system_project					
Product: online_fire_reporting_system					
N/A	02-Jun-22	6.5	Online Fire Reporting System v1.0 is vulnerable to Delete any file via /ofrs/classes/Master.php?f=delete_img.	N/A	A-ONL-ONLI-200622/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31973		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=reports&date=. **CVE ID : CVE-2022-31974**	N/A	A-ONL-ONLI-200622/212
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=user/manage_user&id=. **CVE ID : CVE-2022-31975**	N/A	A-ONL-ONLI-200622/213
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/classes/Master.php?f=delete_request. **CVE ID : CVE-2022-31976**	N/A	A-ONL-ONLI-200622/214
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/classes/Master.php?f=delete_team. **CVE ID : CVE-2022-31977**	N/A	A-ONL-ONLI-200622/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/classes/Master.php?f=delete_inquiry. **CVE ID : CVE-2022-31978**	N/A	A-ONL-ONLI-200622/216
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=teams/manage_team&id=. **CVE ID : CVE-2022-31980**	N/A	A-ONL-ONLI-200622/217
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=teams/view_team&id=. **CVE ID : CVE-2022-31981**	N/A	A-ONL-ONLI-200622/218
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=requests/view_request&id=. **CVE ID : CVE-2022-31982**	N/A	A-ONL-ONLI-200622/219
Improper Neutralization of	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to	N/A	A-ONL-ONLI-200622/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			SQL Injection via /ofrs/admin/?page=requests/manage_request&id=. **CVE ID : CVE-2022-31983**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/requests/take_action.php?id=. **CVE ID : CVE-2022-31984**	N/A	A-ONL-ONLI-200622/221
Vendor: online_market_place_site_project					
Product: online_market_place_site					
Authorization Bypass Through User-Controlled Key	02-Jun-22	4.3	An insecure direct object reference (IDOR) in Online Market Place Site v1.0 allows attackers to modify products that are owned by other sellers. **CVE ID : CVE-2022-29627**	N/A	A-ONL-ONLI-200622/222
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.4	A cross-site scripting (XSS) vulnerability in /omps/seller of Online Market Place Site v1.0 allows attackers to execute arbitrary web cripts or HTML via a crafted payload injected into the Page parameter.	N/A	A-ONL-ONLI-200622/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29628		
Vendor: online_ordering_system_project					
Product: online_ordering_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Ordering System v1.0 by oretnom23 is vulnerable to SQL Injection via admin/editproductetails.php. **CVE ID : CVE-2022-30794**	N/A	A-ONL-ONLI-200622/224
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Ordering System v1.0 by oretnom23 is vulnerable to SQL Injection via admin/editproductimage.php. **CVE ID : CVE-2022-30795**	N/A	A-ONL-ONLI-200622/225
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System 1.0 by oretnom23 is vulnerable to SQL Injection via admin/vieworders.php. **CVE ID : CVE-2022-30797**	N/A	A-ONL-ONLI-200622/226
Improper Neutralization of Special Elements used in an SQL Command	02-Jun-22	7.2	Online Ordering System v1.0 by oretnom23 is vulnerable to SQL Injection via admin/viewreport.php.	N/A	A-ONL-ONLI-200622/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-30798**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Online Ordering System v1.0 by oretnom23 has SQL injection via store/orderpage.php. **CVE ID : CVE-2022-30799**	N/A	A-ONL-ONLI-200622/228
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System By janobe 2.3.2 is vulneranle to SQL Injection via /ordering/index.php?q=products&id=. **CVE ID : CVE-2022-31327**	N/A	A-ONL-ONLI-200622/229
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System By janobe 2.3.2 has SQL Injection via /ordering/admin/products/index.php?view=edit&id=. **CVE ID : CVE-2022-31328**	N/A	A-ONL-ONLI-200622/230
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System By janobe 2.3.2 is vulnerable to SQL Injection via /ordering/admin/orders/loaddata.php. **CVE ID : CVE-2022-31329**	N/A	A-ONL-ONLI-200622/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/stockin/index.php?view=edit&id=. **CVE ID : CVE-2022-31335**	N/A	A-ONL-ONLI-200622/232
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/stockin/loaddata.php. **CVE ID : CVE-2022-31336**	N/A	A-ONL-ONLI-200622/233
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/category/index.php?view=edit&id=. **CVE ID : CVE-2022-31337**	N/A	A-ONL-ONLI-200622/234
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/user/index.php?view=edit&id=. **CVE ID : CVE-2022-31338**	N/A	A-ONL-ONLI-200622/235
Vendor: onlyoffice					
Product: core					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	02-Jun-22	9.8	Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below were discovered to contain a stack overflow via the component DesktopEditor/common/File.cpp. **CVE ID : CVE-2022-29776**	https://github.com/ONLYOFFICE/core/commit/88cf60a3ed4a2b40d71a1c2ced72fa3902a30967	A-ONL-CORE-200622/236
Out-of-bounds Write	02-Jun-22	9.8	Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below were discovered to contain a heap overflow via the component DesktopEditor/fontengine/fontconverter/FontFileBase.h. **CVE ID : CVE-2022-29777**	https://github.com/ONLYOFFICE/core/commit/b17d5e860f30e8be2caeb0022b63be4c76660178	A-ONL-CORE-200622/237
Product: document_server					
Allocation of Resources Without Limits or Throttling	02-Jun-22	9.8	Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below were discovered to contain a stack overflow via the component DesktopEditor/common/File.cpp. **CVE ID : CVE-2022-29776**	https://github.com/ONLYOFFICE/core/commit/88cf60a3ed4a2b40d71a1c2ced72fa3902a30967	A-ONL-DOCU-200622/238
Out-of-bounds Write	02-Jun-22	9.8	Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below	https://github.com/ONLYOFFICE/core/commit/b17d5e860f30	A-ONL-DOCU-200622/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			were discovered to contain a heap overflow via the component DesktopEditor/fontengine/fontconverter/FontFileBase.h. **CVE ID : CVE-2022-29777**	e8be2caeb0022b63be4c76660178	
Vendor: partkeepr					
Product: partkeepr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-22	4.8	A Cross Site Scripting vulnerabilty exists in PartKeepr 1.4.0 via the 'name' field in /api/part_categories. **CVE ID : CVE-2022-30899**	N/A	A-PAR-PART-200622/240
Vendor: Percona					
Product: xtrabackup					
N/A	02-Jun-22	6.5	Percona XtraBackup 2.4.20 unintentionally writes the command line to any resulting backup file output. This may include sensitive arguments passed at run time. In addition, when --history is passed at run time, this command line is also written to the PERCONA_SCHEMA.xtrabackup_history table. NOTE: this issue exists because	https://docs.percona.com/percona-xtrabackup/2.4/release-notes/2.4/2.4.25.html, https://jira.percona.com/browse/PXB-2722	A-PER-XTRA-200622/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of an incomplete fix for CVE-2020-10997. **CVE ID : CVE-2022-26944**		
Vendor: phpabook_project					
Product: phpabook					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	phpABook 0.9i is vulnerable to SQL Injection due to insufficient sanitization of user-supplied data in the "auth_user" parameter in index.php script. **CVE ID : CVE-2022-30352**	N/A	A-PHP-PHPA-200622/242
Vendor: Pidgin					
Product: pidgin					
Improper Certificate Validation	02-Jun-22	5.9	An issue was discovered in Pidgin before 2.14.9. A remote attacker who can spoof DNS responses can redirect a client connection to a malicious server. The client will perform TLS certificate verification of the malicious domain name instead of the original XMPP service domain, allowing the attacker to take over control over the XMPP connection and to obtain user credentials and all	https://github.com/xsf/xeps/pull/1158, https://pidgin.im/about/security/advisories/cve-2022-26491/, https://keep.imfreedom.org/pidgin/pidgin/rev/13cdb7956bdc, https://developer.pidgin.im/wiki/FullChangeLog	A-PID-PIDG-200622/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication content. This is similar to CVE-2022-24968. **CVE ID : CVE-2022-26491**		
Vendor: port389					
Product: 389-ds-base					
Incorrect Authorization	02-Jun-22	7.5	An access control bypass vulnerability found in 389-ds-base. That mishandling of the filter that would yield incorrect results, but as that has progressed, can be determined that it actually is an access control bypass. This may allow any remote unauthenticated user to issue a filter that allows searching for database items they do not have access to, including but not limited to potentially userPassword hashes and other sensitive data. **CVE ID : CVE-2022-1949**	https://bugzilla.redhat.com/show_bug.cgi?id=2091781	A-POR-389--200622/244
Vendor: posix_project					
Product: posix					
Unchecked Return Value	10-Jun-22	7.5	This affects all versions of package posix. When invoking the toString method, it will fallback to 0x0	https://snyk.io/vuln/SNYK-JS-POSIX-2400719	A-POS-POSI-200622/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value, as the value of toString is not invokable (not a function), and then it will crash with type-check. **CVE ID : CVE-2022-21211**		
Vendor: product_show_room_site_project					
Product: product_show_room_site					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	4.8	A vulnerability was found in SourceCodester Product Show Room Site 1.0. It has been declared as problematic. This vulnerability affects p=contact. The manipulation of the Message textbox with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely but requires authentication. Exploit details have been disclosed to the public. **CVE ID : CVE-2022-1979**	N/A	A-PRO-PROD-200622/246
Improper Neutralization of Input During Web Page Generation	02-Jun-22	4.8	A vulnerability was found in SourceCodester Product Show Room Site 1.0. It has been rated as problematic. This issue affects the file	N/A	A-PRO-PROD-200622/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			/admin/?page=system_info/contact_info. The manipulation of the textbox Telephone with the input <script>alert(1)</script> leads to cross site scripting. The attack may be initiated remotely but requires authentication. Exploit details have been disclosed to the public. **CVE ID : CVE-2022-1980**		
Vendor: publiccms					
Product: publiccms					
Exposure of Sensitive Information to an Unauthorized Actor	03-Jun-22	5.3	PublicCMS V4.0.202204.a and below contains an information leak via the component /views/directive/sys/SysConfigDataDirective.java. **CVE ID : CVE-2022-29784**	https://github.com/sanluan/PublicCMS/commit/d8d7626cf51e4968fb384e1637a3c0c9921f33e9	A-PUB-PUBL-200622/248
Vendor: qdecoder_project					
Product: qdecoder					
N/A	03-Jun-22	5.3	qDecoder before 12.1.0 does not ensure that the percent character is followed by two hex digits for URL decoding. **CVE ID : CVE-2022-32265**	https://github.com/wolkykim/qdecoder/pull/29/commits/ce7c8a7ac450a823a11b06508ef1eb7441241f81#diff-1c4e2f5adfa1ad	A-QDE-QDEC-200622/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				30618e78ff459b2c0758ecf34278459ad0a8d58db4fec622ea, https://github.com/wolkykim/qdecoder/pull/29	
Vendor: Realnetworks					
Product: realplayer					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jun-22	9.8	In Real Player 20.0.8.310, the G2 Control allows injection of unsafe javascript: URIs in local HTTP error pages (displayed by Internet Explorer core). This leads to arbitrary code execution. **CVE ID : CVE-2022-32269**	N/A	A-REA-REAL-200622/250
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jun-22	9.8	In Real Player 20.0.7.309 and 20.0.8.310, external::Import() allows download of arbitrary file types and Directory Traversal, leading to Remote Code Execution. This occurs because it is possible to plant executables in the startup folder (DLL planting could also occur). **CVE ID : CVE-2022-32270**	N/A	A-REA-REAL-200622/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-22	9.6	In Real Player 20.0.8.310, there is a DCP:// URI Remote Arbitrary Code Execution Vulnerability. This is an internal URL Protocol used by Real Player to reference a file that contains an URL. It is possible to inject script code to arbitrary domains. It is also possible to reference arbitrary local files. **CVE ID : CVE-2022-32271**	N/A	A-REA-REAL-200622/252
N/A	05-Jun-22	8.8	In Real Player through 20.1.0.312, attackers can execute arbitrary code by placing a UNC share pathname (for a DLL file) in a RAM file. **CVE ID : CVE-2022-32291**	N/A	A-REA-REAL-200622/253
Vendor: Redhat					
Product: directory_server					
Incorrect Authorization	02-Jun-22	7.5	An access control bypass vulnerability found in 389-ds-base. That mishandling of the filter that would yield incorrect results, but as that has progressed, can be determined that it actually is an access control bypass. This	https://bugzilla.redhat.com/show_bug.cgi?id=2091781	A-RED-DIRE-200622/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow any remote unauthenticated user to issue a filter that allows searching for database items they do not have access to, including but not limited to potentially userPassword hashes and other sensitive data. **CVE ID : CVE-2022-1949**		
Product: openshift_container_platform					
Uncontrolled Resource Consumption	07-Jun-22	7.5	A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the Kube API. The ExecSync request runs commands in a container and logs the output of the command. This output is then read by CRI-O after command execution, and it is read in a manner where the entire file corresponding to the output of the command is read in. Thus, if the output of the command is large it is possible to exhaust the memory or the disk space of the node when CRI-O	https://github.com/cri-o/cri-o/commit/f032cf649ecc7e0c46718bd9e7814bfb317cb544	A-RED-OPEN-200622/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reads the output of the command. The highest threat from this vulnerability is system availability. **CVE ID : CVE-2022-1708**		
Vendor: rescue_dispatch_management_system_project					
Product: rescue_dispatch_management_system					
N/A	02-Jun-22	9.1	Rescue Dispatch Management System v1.0 is vulnerable to Delete any file via /rdms/classes/Master.php?f=delete_img. **CVE ID : CVE-2022-31945**	N/A	A-RES-RESC-200622/256
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/classes/Master.php?f=delete_team. **CVE ID : CVE-2022-31946**	N/A	A-RES-RESC-200622/257
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/classes/Master.php?f=delete_report. **CVE ID : CVE-2022-31948**	N/A	A-RES-RESC-200622/258
Improper Neutralization of Special	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via	N/A	A-RES-RESC-200622/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			/rdms/classes/Master.php?f=delete_respondent_type. **CVE ID : CVE-2022-31951**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL injection via /rdms/classes/Master.php?f=delete_incident. **CVE ID : CVE-2022-31952**	N/A	A-RES-RESC-200622/260
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incident_reports/view_report.php?id=. **CVE ID : CVE-2022-31953**	N/A	A-RES-RESC-200622/261
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incident_reports/manage_report.php?id=. **CVE ID : CVE-2022-31956**	N/A	A-RES-RESC-200622/262
Improper Neutralization of Special Elements used in an SQL	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via rdms/admin/teams/view_team.php?id=.	N/A	A-RES-RESC-200622/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2022-31957**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/teams/manage_team.php?id=. **CVE ID : CVE-2022-31959**	N/A	A-RES-RESC-200622/264
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incidents/manage_incident.php?id=. **CVE ID : CVE-2022-31961**	N/A	A-RES-RESC-200622/265
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incidents/view_incident.php?id=. **CVE ID : CVE-2022-31962**	N/A	A-RES-RESC-200622/266
Improper Neutralization of Special Elements used in an SQL Command	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via rdms/admin/respondent_types/view_respondent_type.php?id=.	N/A	A-RES-RESC-200622/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-31964**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/respondent_types/manage_respondent_type.php?id=. **CVE ID : CVE-2022-31965**	N/A	A-RES-RESC-200622/268
Vendor: resi					
Product: gemini-net					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	resi-calltrace in RESI Gemini-Net 4.2 is affected by Multiple XSS issues. Unauthenticated remote attackers can inject arbitrary web script or HTML into an HTTP GET parameter that reflects user input without sanitization. This exists on numerous application endpoints, **CVE ID : CVE-2022-29540**	N/A	A-RES-GEMI-200622/269
Vendor: responsive_online_blog_project					
Product: responsive_online_blog					
Improper Neutralization of Special Elements used in an SQL	02-Jun-22	9.8	Responsive Online Blog v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at single.php.	N/A	A-RES-RESP-200622/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2022-29659**		
Vendor: rosariosis					
Product: rosariosis					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 9.0. **CVE ID : CVE-2022-1997**	https://huntr.dev/bounties/28861ae9-7b09-45b7-a003-eccf903db71d, https://github.com/francoisjacquet/rosariosis/commit/6b22c0b5b40fad891c8cf9e7eeff3e42a35c0bf8	A-ROS-ROSA-200622/271
Vendor: Samsung					
Product: account					
Exposure of Resource to Wrong Sphere	07-Jun-22	7.5	Exposure of Sensitive Information vulnerability in Samsung Account prior to version 13.2.00.6 allows attacker to access sensitive information via onActivityResult. **CVE ID : CVE-2022-30732**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/272
Insertion of Sensitive Information into Log File	07-Jun-22	5.3	Sensitive information exposure in Sign-in log in Samsung Account prior to version 13.2.00.6 allows attackers to get an user email or phone number without permission. **CVE ID : CVE-2022-30733**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	07-Jun-22	5.3	Sensitive information exposure in Sign-out log in Samsung Account prior to version 13.2.00.6 allows attackers to get an user email or phone number without permission. **CVE ID : CVE-2022-30734**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/274
Improper Privilege Management	07-Jun-22	7.5	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get the access_token without permission. **CVE ID : CVE-2022-30735**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/275
Improper Privilege Management	07-Jun-22	5.3	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get the data of contact and gallery without permission. **CVE ID : CVE-2022-30736**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/276
N/A	07-Jun-22	5.3	Implicit Intent hijacking vulnerability in Samsung Account prior to version 13.2.00.6 allows attackers to get email ID.	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30737		
Improper Privilege Management	07-Jun-22	4.3	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get an user email or phone number with a normal level permission. **CVE ID : CVE-2022-30739**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/278
Improper Privilege Management	07-Jun-22	5.3	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get the data of contact and gallery without permission. **CVE ID : CVE-2022-30743**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-ACCO-200622/279
Product: find_my_mobile					
Insertion of Sensitive Information into Log File	07-Jun-22	3.3	Sensitive information exposure vulnerability in SimChangeAlertManger of Find My Mobile prior to 7.2.24.12 allows local attackers with log access permission to get sim card information through device log. **CVE ID : CVE-2022-30741**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-FIND-200622/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	07-Jun-22	3.3	Sensitive information exposure vulnerability in FmmExtraOperation of Find My Mobile prior to 7.2.24.12 allows local attackers with log access permissio to get sim card information through device log. **CVE ID : CVE-2022-30742**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-FIND-200622/281
Product: internet					
Improper Check for Unusual or Exceptional Conditions	07-Jun-22	4.3	Improper check in Loader in Samsung Internet prior to 17.0.1.69 allows attackers to spoof address bar via executing script. **CVE ID : CVE-2022-30738**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-INTE-200622/282
Insecure Storage of Sensitive Information	07-Jun-22	4.3	Improper auto-fill algorithm in Samsung Internet prior to version 17.0.1.69 allows physical attackers to guess stored credit card numbers. **CVE ID : CVE-2022-30740**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-INTE-200622/283
Product: kies					
Uncontrolled Search Path Element	07-Jun-22	7.8	DLL hijacking vulnerability in KiesWrapper in Samsung Kies prior to version 2.6.4.22043_1 allows	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-KIES-200622/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code. **CVE ID : CVE-2022-30744**		
Product: members					
N/A	07-Jun-22	5.5	Unprotected dynamic receiver in Samsung Members prior to version 4.2.005 allows attacker to launch arbitrary activity. **CVE ID : CVE-2022-30748**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-MEMB-200622/285
Product: my_files					
Missing Authorization	07-Jun-22	5.5	Improper access control vulnerability in My Files prior to version 13.1.00.193 allows attackers to access arbitrary private files in My Files application. **CVE ID : CVE-2022-30731**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-MY_F-200622/286
Product: quick_share					
Incorrect Authorization	07-Jun-22	5.5	Improper access control vulnerability in Quick Share prior to version 13.1.2.4 allows attacker to access internal files in Quick Share. **CVE ID : CVE-2022-30745**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-QUIC-200622/287
Product: samsung_pass					
Incorrect Authorization	07-Jun-22	4.6	Improper authorization in Samsung Pass prior to 1.0.00.33 allows	https://security.samsungmobile.com/serviceWe	A-SAM-SAMS-200622/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical attackers to acess account list without authentication. **CVE ID : CVE-2022-30730**	b.smsb?year=2022&month=6	
Product: smartthings					
Exposure of Resource to Wrong Sphere	07-Jun-22	7.5	Missing caller check in Smart Things prior to version 1.7.85.12 allows attacker to access senstive information remotely using javascript interface API. **CVE ID : CVE-2022-30746**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-SMAR-200622/289
Incorrect Default Permissions	07-Jun-22	5.5	PendingIntent hijacking vulnerability in Smart Things prior to 1.7.85.25 allows local attackers to access files without permission via implicit Intent. **CVE ID : CVE-2022-30747**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=6	A-SAM-SMAR-200622/290
Vendor: SAP					
Product: contributor_license_agreement_assistant					
Improper Handling of Exceptional Conditions	06-Jun-22	6.5	Due to improper error handling an authenticated user can crash CLA assistant instance. This could impact the availability of the application. **CVE ID : CVE-2022-29617**	N/A	A-SAP-CONT-200622/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: school_dormitory_management_system_project					
Product: school_dormitory_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	School Dormitory Management System 1.0 is vulnerable to SQL Injection via reports/daily_collection_report.php:59. **CVE ID : CVE-2022-30510**	N/A	A-SCH-SCHO-200622/292
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	School Dormitory Management System 1.0 is vulnerable to SQL Injection via accounts/view_details.php:4. **CVE ID : CVE-2022-30511**	N/A	A-SCH-SCHO-200622/293
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	School Dormitory Management System 1.0 is vulnerable to SQL Injection via accounts/payment_history.php:31. **CVE ID : CVE-2022-30512**	N/A	A-SCH-SCHO-200622/294
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	School Dormitory Management System v1.0 is vulnerable to reflected cross-site scripting (XSS) via admin/inc/navigation.php:125 **CVE ID : CVE-2022-30513**	N/A	A-SCH-SCHO-200622/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	School Dormitory Management System v1.0 is vulnerable to reflected cross-site scripting (XSS) via admin/inc/navigation.php:126. **CVE ID : CVE-2022-30514**	N/A	A-SCH-SCHO-200622/296
Vendor: Seeddms					
Product: seeddms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	5.4	The "Add category" functionality inside the "Global Keywords" menu in "SeedDMS" version 6.0.18 and 5.1.25, is prone to stored XSS which allows an attacker to inject malicious javascript code. **CVE ID : CVE-2022-28051**	https://sourceforge.net/p/seeddms/code/ci/6fc17be5d95e8f00fbe5c124c4acd377fa2ce69d/	A-SEE-SEED-200622/297
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-22	6.5	SeedDMS 6.0.17 and 5.1.24 are vulnerable to Directory Traversal. The "Remove file" functionality inside the "Log files management" menu does not sanitize user input allowing attackers with admin privileges to delete arbitrary files on the remote system. **CVE ID : CVE-2022-28478**	https://github.com/looCiprian/Responsible-Vulnerability-Disclosure/tree/main/CVE-2022-28478, https://sourceforge.net/p/seeddms/code/ci/d68c922152e8a8060dd7fc3ebdd7af685e270e36/	A-SEE-SEED-200622/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-22	4.8	SeedDMS versions 6.0.18 and 5.1.25 and below are vulnerable to stored XSS. An attacker with admin privileges can inject the payload inside the "Role management" menu and then trigger the payload by loading the "Users management" menu **CVE ID : CVE-2022-28479**	https://github.com/looCiprian/Responsible-Vulnerability-Disclosure/tree/main/CVE-2022-28479, https://sourceforge.net/p/seeddms/code/ci/9e92524fdbd1e7c3e6771d669f140c62389ec375/	A-SEE-SEED-200622/299
Vendor: Siemens					
Product: symbia.net					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2),	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	A-SIE-SYMB-200622/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: syngo.via					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	A-SIE-SYNG-200622/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Vendor: simple_bus_ticket_booking_system_project					
Product: simple_bus_ticket_booking_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	9.8	Simple Bus Ticket Booking System 1.0 is vulnerable to SQL Injection via /SimpleBusTicket/index.php. **CVE ID : CVE-2022-30817**	N/A	A-SIM-SIMP-200622/302
Vendor: simple_inventory_system_project					
Product: simple_inventory_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Simple Inventory System v1.0 is vulnerable to SQL Injection via /inventory/login.php. **CVE ID : CVE-2022-31339**	N/A	A-SIM-SIMP-200622/303
Improper Neutralization of Special Elements	02-Jun-22	9.8	Simple Inventory System v1.0 is vulnerable to SQL Injection via	N/A	A-SIM-SIMP-200622/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			/inventory/table_edit_ajax.php. **CVE ID : CVE-2022-31340**		
Vendor: simple_task_scheduling_system_project					
Product: simple_task_scheduling_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-22	9.8	A SQL injection vulnerability exists in Simple Task Scheduling System 1.0 when MySQL is being used as the application database. An attacker can issue SQL commands to the MySQL database through the vulnerable "id" parameter. **CVE ID : CVE-2022-30927**	N/A	A-SIM-SIMP-200622/305
Vendor: solutions-atlantic					
Product: regulatory_reporting_system					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Jun-22	6.5	Solutions Atlantic Regulatory Reporting System (RRS) v500 is vulnerable to Local File Inclusion (LFI). Any authenticated user has the ability to reference internal system files within requests made to the RRSWeb/maint/ShowDocument/ShowDocument.aspx page. The server will successfully respond with the file contents of the internal system file	N/A	A-SOL-REGU-200622/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requested. This ability could allow for adversaries to extract sensitive data and/or files from the underlying file system, gain knowledge about the internal workings of the system, or access source code of the application. **CVE ID : CVE-2022-29597**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Solutions Atlantic Regulatory Reporting System (RRS) v500 is vulnerable to an reflected Cross-Site Scripting (XSS) vulnerability via RRSWeb/maint/ShowDocument/ShowDocument.aspx . **CVE ID : CVE-2022-29598**	N/A	A-SOL-REGU-200622/307
Vendor: sscms					
Product: siteserver_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	siteserver SSCMS 6.15.51 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2022-30349**	N/A	A-SSC-SITE-200622/308
Vendor: starwindsoftware					
Product: starwind_san_\&_nas					
N/A	03-Jun-22	7.2	StarWind SAN and NAS v0.2 build 1914	https://www.starwindsoftware	A-STA-STAR-200622/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow remote code execution. **CVE ID : CVE-2022-32268**	.com/security/sw-20220531-0001/	
Vendor: tigera					
Product: calico_enterprise					
Improper Input Validation	06-Jun-22	5.5	Clusters using Calico (version 3.22.1 and below), Calico Enterprise (version 3.12.0 and below), may be vulnerable to route hijacking with the floating IP feature. Due to insufficient validation, a privileged attacker may be able to set a floating IP annotation to a pod even if the feature is not enabled. This may allow the attacker to intercept and reroute traffic to their compromised pod. **CVE ID : CVE-2022-28224**	https://www.tigera.io/security-bulletins-tta-2022-001/	A-TIG-CALI-200622/310
Vendor: tiktok					
Product: tiktok					
Direct Request ('Forced Browsing')	02-Jun-22	8.8	The TikTok application before 23.8.4 for Android allows account takeover. A crafted URL (unvalidated deeplink) can force the com.zhiliaoapp.music	N/A	A-TIK-TIKT-200622/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ally WebView to load an arbitrary website. This may allow an attacker to leverage an attached JavaScript interface for the takeover with one click. **CVE ID : CVE-2022-28799**		
Vendor: tpcms_project					
Product: tpcms					
Unrestricted Upload of File with Dangerous Type	02-Jun-22	8.8	An arbitrary file upload vulnerability in the Add File function of TPCMS v3.2 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-29624**	N/A	A-TPC-TPCM-200622/312
Vendor: unicorn-engine					
Product: unicorn_engine					
Use After Free	02-Jun-22	7.8	Unicorn Engine v1.0.3 was discovered to contain a use-after-free vulnerability via the hook function. **CVE ID : CVE-2022-29692**	N/A	A-UNI-UNIC-200622/313
Missing Release of Memory after Effective Lifetime	02-Jun-22	7.5	Unicorn Engine v2.0.0-rc7 and below was discovered to contain a memory leak via the function uc_close at /my/unicorn/uc.c.	https://github.com/unicorn-engine/unicorn/commit/469fc4c35a0cfabdbefb158e22d145f4ee6f77b9	A-UNI-UNIC-200622/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29693		
NULL Pointer Dereference	02-Jun-22	7.5	Unicorn Engine v2.0.0-rc7 and below was discovered to contain a NULL pointer dereference via qemu_ram_free. **CVE ID : CVE-2022-29694**	https://github.com/unicorn-engine/unicorn/pull/1593/commits/6a879a082d4d67a5d13f1233ae0334cde0a7f844, https://github.com/unicorn-engine/unicorn/pull/1593/commits/31389e59457f304be3809f9679f91a42daa7ebaa	A-UNI-UNIC-200622/315
Improper Initialization	02-Jun-22	7.5	Unicorn Engine v2.0.0-rc7 contains memory leaks caused by an incomplete unicorn engine initialization. **CVE ID : CVE-2022-29695**	https://github.com/unicorn-engine/unicorn/commit/5a79d7879ca3ee0ce684ad6576d8ac15e8d90fc7	A-UNI-UNIC-200622/316
Vendor: VIM					
Product: vim					
Use After Free	02-Jun-22	7.8	Use After Free in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-1968**	https://huntr.dev/bounties/949090e5-f4ea-4edf-bd79-cd98f0498a5b, https://github.com/vim/vim/commit/409510c588b1eec1ae33511ae97a21eb8e110895	A-VIM-VIM-200622/317
Vendor: webbank					
Product: webcube					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Jun-22	9.8	An issue in Webbank WeCube v3.2.2 allows attackers to execute a directory traversal via a crafted ZIP file. **CVE ID : CVE-2022-28945**	N/A	A-WEB-WEBC-200622/318
Vendor: wedding_management_system_project					
Product: wedding_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL injection via /Wedding-Management/admin/blog_events_edit.php?id=31. **CVE ID : CVE-2022-30818**	N/A	A-WED-WEDD-200622/319
Unrestricted Upload of File with Dangerous Type	02-Jun-22	8.8	In Wedding Management System v1.0, there is an arbitrary file upload vulnerability in the picture upload point of "photos_edit.php" file. **CVE ID : CVE-2022-30819**	N/A	A-WED-WEDD-200622/320
Unrestricted Upload of File with Dangerous Type	02-Jun-22	8.8	In Wedding Management v1.0, there is an arbitrary file upload vulnerability in the picture upload point of "users_edit.php" file. **CVE ID : CVE-2022-30820**	N/A	A-WED-WEDD-200622/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	02-Jun-22	8.8	In Wedding Management System v1.0, the editing function of the "Services" module in the background management system has an arbitrary file upload vulnerability in the picture upload point of "package_edit.php" file. **CVE ID : CVE-2022-30821**	N/A	A-WED-WEDD-200622/322
Unrestricted Upload of File with Dangerous Type	02-Jun-22	8.8	In Wedding Management System v1.0, there is an arbitrary file upload vulnerability in the picture upload point of "users_profile.php" file. **CVE ID : CVE-2022-30822**	N/A	A-WED-WEDD-200622/323
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\blog_events_edit.php. **CVE ID : CVE-2022-30823**	N/A	A-WED-WEDD-200622/324
Improper Neutralization of Special Elements used in an	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\client_edit.php.	N/A	A-WED-WEDD-200622/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			**CVE ID : CVE-2022-30825**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via admin\client_assign.php. **CVE ID : CVE-2022-30826**	N/A	A-WED-WEDD-200622/326
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\package_edit.php. **CVE ID : CVE-2022-30827**	N/A	A-WED-WEDD-200622/327
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\photos_edit.php. **CVE ID : CVE-2022-30828**	N/A	A-WED-WEDD-200622/328
Improper Neutralization of Special Elements used in an SQL Command	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\users_edit.php. **CVE ID : CVE-2022-30829**	N/A	A-WED-WEDD-200622/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\feature_edit.php. **CVE ID : CVE-2022-30830**	N/A	A-WED-WEDD-200622/330
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via Wedding-Management/wedding_details.php. **CVE ID : CVE-2022-30831**	N/A	A-WED-WEDD-200622/331
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via /Wedding-Management/admin/client_assign.php?booking=31&user_id=. **CVE ID : CVE-2022-30832**	N/A	A-WED-WEDD-200622/332
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via /Wedding-Management/admin/client_edit.php?booking=31&user_id=. **CVE ID : CVE-2022-30833**	N/A	A-WED-WEDD-200622/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection via /Wedding-Management/admin/client_manage_account_details.php?booking_id=31&user_id= **CVE ID : CVE-2022-30834**	N/A	A-WED-WEDD-200622/334
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection. via /Wedding-Management/admin/budget.php?booking_id=. **CVE ID : CVE-2022-30835**	N/A	A-WED-WEDD-200622/335
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-22	7.2	Wedding Management System v1.0 is vulnerable to SQL Injection. via Wedding-Management/admin/select.php. **CVE ID : CVE-2022-30836**	N/A	A-WED-WEDD-200622/336
Vendor: winaprs					
Product: winaprs					
Buffer Copy without Checking Size of Input ('Classic	02-Jun-22	7.5	** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered in WinAPRS 2.9.0. A buffer overflow in DIGI address processing for VHF KISS packets allows a	https://winaprs.com/	A-WIN-WINA-200622/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote attacker to cause a denial of service (daemon crash) via a malicious AX.25 packet over the air. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-24700**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jun-22	7.8	** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered in WinAPRS 2.9.0. A buffer overflow in national.txt processing allows a local attacker to cause a denial of service or possibly achieve code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-24701**	N/A	A-WIN-WINA-200622/338
Buffer Copy without Checking Size of Input ('Classic	02-Jun-22	9.8	** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered in WinAPRS 2.9.0. A buffer overflow in the VHF KISS TNC component allows a remote attacker to	https://winaprs.com/	A-WIN-WINA-200622/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			achieve remote code execution via malicious AX.25 packets over the air. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-24702**		
Vendor: xuxueli					
Product: xxl-job					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-22	5.4	XXL-Job v2.3.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via /xxl-job-admin/jobinfo. **CVE ID : CVE-2022-29770**	N/A	A-XUX-XXL--200622/340
Hardware					
Vendor: BD					
Product: pyxis_anesthesia_station_es					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_ciisafe					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_logistics					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/343
Product: pyxis_medbank					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-	H-BD-PYXI-200622/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	default-credentials	
Product: pyxis_medstation_4000					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types.	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_medstation_es					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information.	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22767		
Product: pyxis_medstation_es_server					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/347
Product: pyxis_parassist					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_rapid_rx					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_stockstation					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/350
Product: pyxis_supplycenter					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/351
Product: pyxis_supplyroller					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_supplystation					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_supplystation_ec					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-PYXI-200622/354
Product: pyxis_supplystation_rf_auxiliary					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may	https://cybersecurity.bd.com/bulletins-and-patches/bd-	H-BD-PYXI-200622/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	pyxis-products-default-credentials	
Product: rowa_pouch_packaging_systems					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	H-BD-ROWA-200622/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Vendor: Dell					
Product: powerstore_t					
Uncontrolled Resource Consumption	02-Jun-22	7.5	Dell PowerStore contains an Uncontrolled Resource Consumption Vulnerability in PowerStore User Interface. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the Denial of Service. **CVE ID : CVE-2022-22556**	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/357
Improper Authentication	02-Jun-22	7.8	PowerStore contains Plain-Text Password Storage Vulnerability in PowerStore X & T environments running versions 2.0.0.x and 2.0.1.x A locally authenticated attacker could potentially exploit	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account. **CVE ID : CVE-2022-22557**		
Improper Neutralization of Formula Elements in a CSV File	02-Jun-22	8	PowerStore SW v2.1.1.0 supports the option to export data to either a CSV or an XLSX file. The data is taken as is, without any validation or sanitization. It allows a malicious, authenticated user to inject payloads that might get interpreted as formulas by the corresponding spreadsheet application that is being used to open the CSV/XLSX file. **CVE ID : CVE-2022-26867**	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/359
Improper Neutralization of Special Elements used in an OS Command	02-Jun-22	7.8	Dell EMC PowerStore versions 2.0.0.x, 2.0.1.x, and 2.1.0.x are vulnerable to a command injection flaw. An authenticated	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system takeover by an attacker. **CVE ID : CVE-2022-26868**		
Exposure of Resource to Wrong Sphere	02-Jun-22	9.8	Dell PowerStore versions 2.0.0.x, 2.0.1.x and 2.1.0.x contains an open port vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure and arbitrary code execution. **CVE ID : CVE-2022-26869**	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/361
Product: powerstore_x					
Uncontrolled Resource Consumption	02-Jun-22	7.5	Dell PowerStore contains an Uncontrolled Resource Consumption Vulnerability in	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PowerStore User Interface. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the Denial of Service. **CVE ID : CVE-2022-22556**		
Improper Authentication	02-Jun-22	7.8	PowerStore contains Plain-Text Password Storage Vulnerability in PowerStore X & T environments running versions 2.0.0.x and 2.0.1.x A locally authenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account. **CVE ID : CVE-2022-22557**	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/363
Improper Neutralization of Formula Elements in a CSV File	02-Jun-22	8	PowerStore SW v2.1.1.0 supports the option to export data to either a CSV or an XLSX file. The data is taken as is, without any validation or sanitization. It allows a malicious,	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to inject payloads that might get interpreted as formulas by the corresponding spreadsheet application that is being used to open the CSV/XLSX file. **CVE ID : CVE-2022-26867**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Jun-22	7.8	Dell EMC PowerStore versions 2.0.0.x, 2.0.1.x, and 2.1.0.x are vulnerable to a command injection flaw. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system takeover by an attacker. **CVE ID : CVE-2022-26868**	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/365
Exposure of Resource	02-Jun-22	9.8	Dell PowerStore versions 2.0.0.x, 2.0.1.x and 2.1.0.x contains an open port vulnerability. A	https://www.dell.com/support/kbdoc/000196367	H-DEL-POWE-200622/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure and arbitrary code execution. **CVE ID : CVE-2022-26869**		
Vendor: deltacontrols					
Product: entelitouch					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 was discovered to contain a cross-site scripting (XSS) vulnerability via the Username parameter. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-29732**	https://www.deltacontrols.com/	H-DEL-ENTE-200622/367
Cleartext Transmission of Sensitive Information	02-Jun-22	5.9	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 was discovered to transmit and store sensitive information in cleartext. This	https://www.deltacontrols.com/	H-DEL-ENTE-200622/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to intercept HTTP Cookie authentication credentials via a man-in-the-middle attack. **CVE ID : CVE-2022-29733**		
Cross-Site Request Forgery (CSRF)	02-Jun-22	8.8	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 allows attackers to execute arbitrary commands via a crafted HTTP request. **CVE ID : CVE-2022-29735**	https://www.deltacontrols.com/	H-DEL-ENTE-200622/369
Vendor: Dlink					
Product: dir-890l					
N/A	03-Jun-22	8.8	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-890L 1.20b01 allows attackers to execute arbitrary code due to the hardcoded option Wake-On-Lan for the parameter 'descriptor' at SetVirtualServerSettings.php. **CVE ID : CVE-2022-29778**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--200622/370
Out-of-bounds Write	02-Jun-22	9.8	The LAN-side Web-Configuration Interface has Stack-based Buffer	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--200622/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Overflow vulnerability in the D-Link Wi-Fi router firmware DIR-890L DIR890LA1_FW107b09.bin and previous versions. The function created at 0x17958 of /htdocs/cgibin will call sprintf without checking the length of strings in parameters given by HTTP header and can be controlled by users easily. The attackers can exploit the vulnerability to carry out arbitrary code by means of sending a specially constructed payload to port 49152. **CVE ID : CVE-2022-30521**		
Vendor: H3C					
Product: magic_r100					
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the CMD parameter at /goform/aspForm. **CVE ID : CVE-2022-30909**	N/A	H-H3C-MAGI-200622/372
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack	N/A	H-H3C-MAGI-200622/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow vulnerability via the GO parameter at /goform/aspForm. **CVE ID : CVE-2022-30910**		
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateWanParams parameter at /goform/aspForm. **CVE ID : CVE-2022-30912**	N/A	H-H3C-MAGI-200622/374
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the ipqos_set_bandwidth parameter at /goform/aspForm. **CVE ID : CVE-2022-30913**	N/A	H-H3C-MAGI-200622/375
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateMacClone parameter at /goform/aspForm. **CVE ID : CVE-2022-30914**	N/A	H-H3C-MAGI-200622/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateSnat parameter at /goform/aspForm. **CVE ID : CVE-2022-30915**	N/A	H-H3C-MAGI-200622/377
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTelnetDebug parameter at /goform/aspForm. **CVE ID : CVE-2022-30916**	N/A	H-H3C-MAGI-200622/378
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the AddWlanMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30917**	N/A	H-H3C-MAGI-200622/379
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTelnet parameter at /goform/aspForm.	N/A	H-H3C-MAGI-200622/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30918		
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Edit_BasicSSID_5G parameter at /goform/aspForm. **CVE ID : CVE-2022-30919**	N/A	H-H3C-MAGI-200622/381
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Edit_BasicSSID parameter at /goform/aspForm. **CVE ID : CVE-2022-30920**	N/A	H-H3C-MAGI-200622/382
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the SetMobileAPInfoById parameter at /goform/aspForm. **CVE ID : CVE-2022-30921**	N/A	H-H3C-MAGI-200622/383
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the EditWlanMacList	N/A	H-H3C-MAGI-200622/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at /goform/aspForm. **CVE ID : CVE-2022-30922**		
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTimingtime WifiAndLed parameter at /goform/aspForm. **CVE ID : CVE-2022-30923**	N/A	H-H3C-MAGI-200622/385
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the SetAPWifiorLedInfo ById parameter at /goform/aspForm. **CVE ID : CVE-2022-30924**	N/A	H-H3C-MAGI-200622/386
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the AddMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30925**	N/A	H-H3C-MAGI-200622/387
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to	N/A	H-H3C-MAGI-200622/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow vulnerability via the EditMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30926**		
Vendor: ict					
Product: protege_gx					
Use of Password Hash With Insufficient Computational Effort	02-Jun-22	4.3	An access control issue in ICT Protege GX/WX 2.08 allows attackers to leak SHA1 password hashes of other users. **CVE ID : CVE-2022-29731**	https://www.ict.co/	H-ICT-PROT-200622/389
Product: protege_wx					
Use of Password Hash With Insufficient Computational Effort	02-Jun-22	4.3	An access control issue in ICT Protege GX/WX 2.08 allows attackers to leak SHA1 password hashes of other users. **CVE ID : CVE-2022-29731**	https://www.ict.co/	H-ICT-PROT-200622/390
Vendor: keysight					
Product: n6841a_rf					
Deserialization of Untrusted Data	02-Jun-22	9.8	The affected products are vulnerable of untrusted data due to deserialization without prior authorization/authentication, which may allow an attacker to	N/A	H-KEY-N684-200622/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely execute arbitrary code. **CVE ID : CVE-2022-1660**		
Relative Path Traversal	02-Jun-22	7.5	The affected products are vulnerable to directory traversal, which may allow an attacker to obtain arbitrary operating system files. **CVE ID : CVE-2022-1661**	N/A	H-KEY-N684-200622/392
Product: n6854a					
Deserialization of Untrusted Data	02-Jun-22	9.8	The affected products are vulnerable of untrusted data due to deserialization without prior authorization/authentication, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2022-1660**	N/A	H-KEY-N685-200622/393
Relative Path Traversal	02-Jun-22	7.5	The affected products are vulnerable to directory traversal, which may allow an attacker to obtain arbitrary operating system files. **CVE ID : CVE-2022-1661**	N/A	H-KEY-N685-200622/394
Vendor: mediatek					
Product: mt6580					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT65-200622/395
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT65-200622/396
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT65-200622/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT65-200622/398
Product: mt6731					
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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/June-2022	H-MED-MT67-200622/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Product: mt6732					
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/400
Product: mt6735					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/402
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/404
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/405
Product: mt6737					
Incorrect Permission Assignment for	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/407
Product: mt6739					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/409
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/411
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/412
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory	https://corp.mediatek.com/pro	H-MED-MT67-200622/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	duct-security-bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/414
Product: mt6750					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/416
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Product: mt6750s					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/418
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/420
Product: mt6752					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/421
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/423
Product: mt6753					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/425
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/427
Product: mt6755					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/429
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/430
Product: mt6755s					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/432
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Product: mt6757					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/434
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21755		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/436
Product: mt6757c					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/437
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read	https://corp.mediatek.com/product-security-	H-MED-MT67-200622/438

Weakness	Publish Date	CVSSv3	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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	bulletin/June-2022	
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/439
Product: mt6757cd					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/441
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Product: mt6757ch					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/443
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/445
Product: mt6758					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/446
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/448
Product: mt6761					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/450
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/452
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/454
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/455
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/457
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/459
Product: mt6762					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21745		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/461
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/462
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read	https://corp.mediatek.com/product-security-	H-MED-MT67-200622/463

Weakness	Publish Date	CVSSv3	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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	bulletin/June-2022	
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/464
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt6763					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/466
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21755		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/468
Product: mt6765					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/470
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/471
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-200622/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/473
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/475
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/477
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/478
Product: mt6768					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/480
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/482
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/484
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/485
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory	https://corp.mediatek.com/pro	H-MED-MT67-200622/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	duct-security-bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/487
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt6769					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/489
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/491
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/493
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/494
Product: mt6771					
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/496
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/498
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/500
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/501
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/503
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Product: mt6779					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/505
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21746		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/507
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/508
Incorrect Permission Assignment for	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-200622/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/510
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/512
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21754		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/514
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/515
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/517
Product: mt6781					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/519
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/521
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/523
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/524
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/526
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/528
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/529
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT67-200622/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt6785					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/531
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/533
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/535
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/537
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/538
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/540
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/542
Product: mt6789					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21745		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/544
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/545
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-200622/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	bulletin/June-2022	
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/547
Product: mt6795					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/549
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21758		
Product: mt6797					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/551
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/552
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory	https://corp.mediatek.com/pro	H-MED-MT67-200622/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	duct-security-bulletin/June-2022	
Product: mt6799					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/554
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT67-200622/556
Product: mt6833					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/558
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21747		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/560
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/562
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/563
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/565
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/567
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/568
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/570
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt6853					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/572
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/574
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/575
Incorrect Permission	06-Jun-22	5.5	In telephony, there is a possible	https://corp.mediatek.com/pro	H-MED-MT68-200622/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	duct-security-bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/577
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, 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/June-2022	H-MED-MT68-200622/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/579
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/581
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/582
Improper Validation	06-Jun-22	7.5	In WIFI Firmware, there is a possible	https://corp.mediatek.com/pro	H-MED-MT68-200622/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Integrity Check Value			system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	duct-security-bulletin/June-2022	
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/584
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/586
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/588
Product: mt6853t					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/589
Incorrect Permission	06-Jun-22	5.5	In telephony, there is a possible	https://corp.mediatek.com/pro	H-MED-MT68-200622/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	duct-security-bulletin/June-2022	
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/591
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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/June-2022	H-MED-MT68-200622/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/593
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21760		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/595
Product: mt6873					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/597
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/598
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/600
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/602
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/604
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/605
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/607
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/609
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/610
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	bulletin/June-2022	
Product: mt6875					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/612
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/614
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/616
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/618
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/619
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/621
Product: mt6877					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/623
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/625
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/627
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/628
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/630
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/632
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/633
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	bulletin/June-2022	
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/635
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**		
Product: mt6879					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/637
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/639
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/641
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/642
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/644
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/646
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/647
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt6880					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/649
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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/June-2022	H-MED-MT68-200622/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/651
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Product: mt6883					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/653
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/655
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/657
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/658
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/660
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/662
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/663
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/665
Product: mt6885					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/667
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/669
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/671
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/672
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/674
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/676
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/677
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/679
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/681
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/682
Product: mt6889					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/683
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/685
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/686
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/688
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/690
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/692
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/693
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/695
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6890					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/697
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/698
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	bulletin/June-2022	
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/700
Product: mt6891					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/702
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/704
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/706
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/707
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/709
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21762		
Product: mt6893					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/711
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/713
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/714
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/716
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/718
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/720
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/721
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/723
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/725
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/726
Product: mt6895					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	bulletin/June-2022	
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/728
Incorrect Permission Assignment for	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/730
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/732
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21754		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/734
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/735
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This	https://corp.mediatek.com/product-security-	H-MED-MT68-200622/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/737
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT68-200622/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt6983					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/739
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/741
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/743
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/744
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/746
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/748
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/749
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT69-200622/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt6985					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/751
Incorrect Permission Assignment for	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/753
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/755
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT69-200622/756
Product: mt8167					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/757
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/758
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Product: mt8167s					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/760
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/762
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/764
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/765
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/767
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/769
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/770
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write	https://corp.mediatek.com/product-security-	H-MED-MT81-200622/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	bulletin/June-2022	
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/772
Product: mt8168					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/774
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/776
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/778
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/779
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/781
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/783
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/784
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT81-200622/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt8173					
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/786
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Product: mt8175					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/788
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/790
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/792
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/793
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/795
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/797
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/798
Product: mt8183					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption	https://corp.mediatek.com/product-security-	H-MED-MT81-200622/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/800
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/802
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/804
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/806
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/807
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt8185					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/809
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/811
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21752		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/813
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/814
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect	https://corp.mediatek.com/product-security-	H-MED-MT81-200622/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	bulletin/June-2022	
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/816
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/818
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT81-200622/819
Product: mt8321					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/820
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/821
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT83-200622/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/823
Product: mt8362a					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/825
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/827
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/829
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/830
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/832
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/834
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/835
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT83-200622/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt8365					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/837
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/839
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/841
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/843
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/844
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/846
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/848
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/849
Product: mt8385					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/850
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/852
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/853
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/855
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/857
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/858
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write	https://corp.mediatek.com/product-security-	H-MED-MT83-200622/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	bulletin/June-2022	
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT83-200622/860
Product: mt8666					
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/862
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/864
Product: mt8667					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/866
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/868
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/869
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/871
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/873
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/874
Product: mt8675					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption	https://corp.mediatek.com/product-security-	H-MED-MT86-200622/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	bulletin/June-2022	
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/876
Incorrect Permission Assignment for	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission	https://corp.mediatek.com/product-security-	H-MED-MT86-200622/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/878
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/880
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21753		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/882
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/883
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect	https://corp.mediatek.com/product-security-	H-MED-MT86-200622/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	bulletin/June-2022	
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/885
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/887
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/888
Product: mt8695					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/889
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/891
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/892
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/894
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt8696					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/896
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/898
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/900
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/901
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT86-200622/903
Product: mt8765					
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/905
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/907
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/908
Product: mt8766					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/910
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/912
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/914
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/916
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/917
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/919
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/921
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/922
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT87-200622/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt8768					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/924
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/926
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/928
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21751		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/930
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/931
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	H-MED-MT87-200622/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	bulletin/June-2022	
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/933
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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/June-2022	H-MED-MT87-200622/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/935
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/937
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/938
Product: mt8786					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/940
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/942
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/944
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/946
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/947
Out-of-bounds Read	06-Jun-22	4.4	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/949
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/951
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/952
Integer Overflow or	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to	https://corp.mediatek.com/product-security-	H-MED-MT87-200622/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	bulletin/June-2022	
Product: mt8788					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/954
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/956
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/958
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/960
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/961
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/963
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/965
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/966
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-security-	H-MED-MT87-200622/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/968
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt8789					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/970
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/972
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/974
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/975
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/977
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/979
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/980
Improper Validation	06-Jun-22	7.5	In WIFI Firmware, there is a possible	https://corp.mediatek.com/pro	H-MED-MT87-200622/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Integrity Check Value			system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	duct-security-bulletin/June-2022	
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/982
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/984
Product: mt8791					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/986
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058.	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21749		
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/988
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/989
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**		
Product: mt8797					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/991
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**		
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/993
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission 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/June-2022	H-MED-MT87-200622/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/995
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/997
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/998
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**		
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/1000
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950;	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**		
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/1002
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/1003
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	H-MED-MT87-200622/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	bulletin/June-2022	
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT87-200622/1005
Product: mt9636					
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT96-200622/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT96-200622/1007
Product: mt9638					
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT96-200622/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT96-200622/1009
Product: mt9666					
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562. **CVE ID : CVE-2022-21760**	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT96-200622/1010
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System	https://corp.mediatek.com/product-security-bulletin/June-2022	H-MED-MT96-200622/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**		
Vendor: Netapp					
Product: hci_compute_node					
Cleartext Transmission of Sensitive Information	02-Jun-22	4.3	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP step even when HTTP is provided in theURL. This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when it built the HSTS cache. Or the otherway around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL. **CVE ID : CVE-2022-30115**	https://security.netapp.com/advisory/ntap-20220609-0009/	H-NET-HCI_-200622/1012
Vendor: owllabs					
Product: meeting_owl_pro					
Exposure of Sensitive	02-Jun-22	6.5	Owl Labs Meeting Owl 5.2.0.15 allows	N/A	H-OWL-MEET-200622/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			attackers to retrieve the passcode hash via a certain c 10 value over Bluetooth. **CVE ID : CVE-2022-31459**		
Use of Hard-coded Credentials	02-Jun-22	7.4	Owl Labs Meeting Owl 5.2.0.15 allows attackers to activate Tethering Mode with hard-coded hoothoot credentials via a certain c 150 value. **CVE ID : CVE-2022-31460**	N/A	H-OWL-MEET-200622/1014
Improper Authentication	02-Jun-22	6.5	Owl Labs Meeting Owl 5.2.0.15 allows attackers to deactivate the passcode protection mechanism via a certain c 11 message. **CVE ID : CVE-2022-31461**	N/A	H-OWL-MEET-200622/1015
Use of Hard-coded Credentials	02-Jun-22	8.8	Owl Labs Meeting Owl 5.2.0.15 allows attackers to control the device via a backdoor password (derived from the serial number) that can be found in Bluetooth broadcast data. **CVE ID : CVE-2022-31462**	N/A	H-OWL-MEET-200622/1016
Improper Authentication	02-Jun-22	7.1	Owl Labs Meeting Owl 5.2.0.15 does not require a password for Bluetooth	N/A	H-OWL-MEET-200622/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands, because only client-side authentication is used. **CVE ID : CVE-2022-31463**		
Vendor: Rockwellautomation					
Product: compactlogix_5370					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	H-ROC-COMP-200622/1018
Product: compactlogix_5380					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answe	H-ROC-COMP-200622/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	r_view/a_id/1135559	
Product: compactlogix_5480					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	H-ROC-COMP-200622/1020
Product: compact_guardlogix_5370					
Uncontrolled Resource	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01,	H-ROC-COMP-200622/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	
Product: compact_guardlogix_5380					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	H-ROC-COMP-200622/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1797		
Product: controllogix_5570					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	H-ROC-CONT-200622/1023
Product: controllogix_5580					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	H-ROC-CONT-200622/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**		
Product: guardlogix_5570					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	H-ROC-GUAR-200622/1025
Product: guardlogix_5580					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answe	H-ROC-GUAR-200622/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	r_view/a_id/1135559	
Vendor: Schneider-electric					
Product: powerlogic_ion_setup					
Improper Input Validation	02-Jun-22	8.8	A CWE-20: Improper Input Validation vulnerability exists that could cause potential remote code execution when an attacker is able to intercept and modify a request on the same network or has configuration access to an ION device on the network. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30232**	https://www.se.com/ww/en/download/document/SEVD-2022-130-01/	H-SCH-POWE-200622/1027
Product: wiser_smart_eer21000					
Improper Input Validation	02-Jun-22	6.5	A CWE-20: Improper Input Validation vulnerability exists that could allow the product to be	https://www.se.com/ww/en/download/docu	H-SCH-WISE-200622/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously manipulated when the user is tricked into performing certain actions on a webpage. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30233**	ment/SEVD-2022-130-03/	
Use of Hard-coded Credentials	02-Jun-22	9.8	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could allow arbitrary code to be executed when root level access is obtained. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30234**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1029
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow unauthorized access when an attacker uses brute force. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30235		
Incorrect Resource Transfer Between Spheres	02-Jun-22	8.2	A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could allow unauthorized access when an attacker uses cross-domain attacks. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30236**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1031
Missing Encryption of Sensitive Data	02-Jun-22	7.5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow authentication credentials to be recovered when an attacker breaks the encoding. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30237**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1032
Improper Authentication	02-Jun-22	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow an attacker to take over the admin account when an attacker	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hijacks a session. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30238**		
Product: wiser_smart_eer21001					
Improper Input Validation	02-Jun-22	6.5	A CWE-20: Improper Input Validation vulnerability exists that could allow the product to be maliciously manipulated when the user is tricked into performing certain actions on a webpage. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30233**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1034
Use of Hard-coded Credentials	02-Jun-22	9.8	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could allow arbitrary code to be executed when root level access is obtained. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30234**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow unauthorized access when an attacker uses brute force. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30235**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1036
Incorrect Resource Transfer Between Spheres	02-Jun-22	8.2	A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could allow unauthorized access when an attacker uses cross-domain attacks. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30236**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1037
Missing Encryption of Sensitive Data	02-Jun-22	7.5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow authentication credentials to be recovered when an attacker breaks the encoding. Affected	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30237**		
Improper Authentication	02-Jun-22	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow an attacker to take over the admin account when an attacker hijacks a session. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30238**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	H-SCH-WISE-200622/1039
Vendor: Siemens					
Product: biograph_horizon_pet\/ct_systems					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-BIOG-200622/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: magnetom_numaris_x					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2),	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-MAGN-200622/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: mammomat_revelation					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-MAMM-200622/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: naeotom_alpha					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-NAEO-200622/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.all					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2),	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.now					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.open_pro					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.sim					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.up					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_x.cite					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_x.creed					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SOMA-200622/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_e					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SYMB-200622/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_evo					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SYMB-200622/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_intevo					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SYMB-200622/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_s					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SYMB-200622/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_t					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	H-SIE-SYMB-200622/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Vendor: Tenda					
Product: hg6					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Jun-22	8.8	Tenda Technology Co.,Ltd HG6 3.3.0-210926 was discovered to contain a command injection vulnerability via the pingAddr and traceAddr parameters. This vulnerability is exploited via a crafted POST request. **CVE ID : CVE-2022-30425**	https://www.tendacn.com/	H-TEN-HG6-200622/1056
Vendor: usr					
Product: usr-g800v2					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	H-USR-USR--200622/1057
Product: usr-g806					
Use of Hard-	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to	https://www.pusr.com/	H-USR-USR--200622/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**		
Product: usr-g807					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	H-USR-USR--200622/1059
Product: usr-g808					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	H-USR-USR--200622/1060
Product: usr-lg220-l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	H-USR-USR--200622/1061
Vendor: Verizon					
Product: 4g_lte_network_extender					
Weak Password Requirements	02-Jun-22	7.5	Verizon 4G LTE Network Extender GA4.38 - V0.4.038.2131 utilizes a weak default admin password generation algorithm which generates passwords that are accessible to unauthenticated attackers via the webUI login page. **CVE ID : CVE-2022-29729**	https://www.verizon.com/	H-VER-4G_L-200622/1062
Vendor: Watchguard					
Product: fireboxcloud					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: fireboxv					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1064
Product: firebox_m200					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_m270					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1066
Product: firebox_m290					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25361		
Product: firebox_m300					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1068
Product: firebox_m370					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1069
Product: firebox_m390					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1070
Product: firebox_m400					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1071
Product: firebox_m440					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated	https://www.watchguard.com/wgrd-psirt/advisory/	H-WAT-FIRE-200622/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	wgsa-2022-00004, https://watchguard.com	
Product: firebox_m470					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1073
Product: firebox_m4800					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_m500					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1075
Product: firebox_m570					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_m5800					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1077
Product: firebox_m590					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25361		
Product: firebox_m670					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1079
Product: firebox_m690					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1080
Product: firebox_t10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1081
Product: firebox_t10-d					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1082
Product: firebox_t10-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated	https://www.watchguard.com/wgrd-psirt/advisory/	H-WAT-FIRE-200622/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	wgsa-2022-00004, https://watchguard.com	
Product: firebox_t15					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1084
Product: firebox_t15-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_t20					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1086
Product: firebox_t20-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_t30					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1088
Product: firebox_t30-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25361		
Product: firebox_t35					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1090
Product: firebox_t35-r					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1091
Product: firebox_t35-w					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1092
Product: firebox_t40					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1093
Product: firebox_t40-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated	https://www.watchguard.com/wgrd-psirt/advisory/	H-WAT-FIRE-200622/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	wgsa-2022-00004, https://watchguard.com	
Product: firebox_t50					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1095
Product: firebox_t50-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_t55					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1097
Product: firebox_t55-w					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: firebox_t70					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1099
Product: firebox_t80					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25361		
Product: firebox_xtm1520-rp					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1101
Product: firebox_xtm1525-rp					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1102
Product: firebox_xtm2520					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1103
Product: firebox_xtm850					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1104
Product: firebox_xtm860					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated	https://www.watchguard.com/wgrd-psirt/advisory/	H-WAT-FIRE-200622/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	wgsa-2022-00004, https://watchguard.com	
Product: firebox_xtm870					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1106
Product: firebox_xtm870-f					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-FIRE-200622/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**		
Product: xtmv					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	H-WAT-XTMV-200622/1108
Operating System					
Vendor: Apple					
Product: iphone_os					
Use of Hard-coded Credentials	02-Jun-22	9.8	LinkPlay Sound Bar v1.0 allows attackers to escalate privileges via a hardcoded password for the SSL certificate. **CVE ID : CVE-2022-28605**	N/A	O-APP-IPHO-200622/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: BD					
Product: pyxis_anesthesia_station_es_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1110
Product: pyxis_ciisafe_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_logistics_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_medbank_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1113
Product: pyxis_medstation_4000_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1114
Product: pyxis_medstation_es_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_medstation_es_server_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_parassist_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1117
Product: pyxis_rapid_rx_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may	https://cybersecurity.bd.com/bulletins-and-patches/bd-	O-BD-PYXI-200622/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	pyxis-products-default-credentials	
Product: pyxis_stockstation_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_supplycenter_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information.	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22767		
Product: pyxis_supplyroller_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1121
Product: pyxis_supplystation_ec_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_supplystation_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**		
Product: pyxis_supplystation_rf_auxiliary_firmware					
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-PYXI-200622/1124
Product: rowa_pouch_packaging_systems_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	02-Jun-22	8.8	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information. **CVE ID : CVE-2022-22767**	https://cybersecurity.bd.com/bulletins-and-patches/bd-pyxis-products-default-credentials	O-BD-ROWA-200622/1125
Vendor: Debian					
Product: debian_linux					
Improper Certificate Validation	02-Jun-22	5.9	An issue was discovered in Pidgin before 2.14.9. A remote attacker who can spoof DNS responses can redirect a client connection to a malicious server. The client will perform TLS	https://github.com/xsf/xeps/pull/1158, https://pidgin.im/about/security/advisories/cve-2022-26491/, https://keep.imfreedom.org/pidgin/pidgin/rev	O-DEB-DEBI-200622/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certificate verification of the malicious domain name instead of the original XMPP service domain, allowing the attacker to take over control over the XMPP connection and to obtain user credentials and all communication content. This is similar to CVE-2022-24968. **CVE ID : CVE-2022-26491**	/13cdb7956bdc, https://developer.pidgin.im/wiki/FullChangeLog	
Improper Handling of Exceptional Conditions	02-Jun-22	9.8	Bottle before 0.12.20 mishandles errors during early request binding. **CVE ID : CVE-2022-31799**	https://github.com/bottlepy/bottle/commit/e140e1b54da721a660f2eb9d58a106b7b3ff2f00, https://github.com/bottlepy/bottle/commit/a2b0ee6bb4ce88895429ec4aca856616244c4c4c	O-DEB-DEBI-200622/1127
Vendor: Dell					
Product: powerstoreos					
Uncontrolled Resource Consumption	02-Jun-22	7.5	Dell PowerStore contains an Uncontrolled Resource Consumption Vulnerability in PowerStore User Interface. A remote unauthenticated attacker could	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-200622/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability, leading to the Denial of Service. **CVE ID : CVE-2022-22556**		
Improper Authentication	02-Jun-22	7.8	PowerStore contains Plain-Text Password Storage Vulnerability in PowerStore X & T environments running versions 2.0.0.x and 2.0.1.x A locally authenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account. **CVE ID : CVE-2022-22557**	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-200622/1129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	5.5	Dell PowerStore Versions before v2.1.1.0. contains a Stored Cross-Site Scripting vulnerability. A high privileged network attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-200622/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery. **CVE ID : CVE-2022-26866**		
Improper Neutralization of Formula Elements in a CSV File	02-Jun-22	8	PowerStore SW v2.1.1.0 supports the option to export data to either a CSV or an XLSX file. The data is taken as is, without any validation or sanitization. It allows a malicious, authenticated user to inject payloads that might get interpreted as formulas by the corresponding spreadsheet application that is being used to open the CSV/XLSX file. **CVE ID : CVE-2022-26867**	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-200622/1131
Improper Neutralization of	02-Jun-22	7.8	Dell EMC PowerStore versions 2.0.0.x, 2.0.1.x, and	https://www.dell.com/support	O-DEL-POWE-200622/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			2.1.0.x are vulnerable to a command injection flaw. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system takeover by an attacker. **CVE ID : CVE-2022-26868**	/kbdoc/000196367	
Exposure of Resource to Wrong Sphere	02-Jun-22	9.8	Dell PowerStore versions 2.0.0.x, 2.0.1.x and 2.1.0.x contains an open port vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure and arbitrary code execution. **CVE ID : CVE-2022-26869**	https://www.dell.com/support/kbdoc/000196367	O-DEL-POWE-200622/1133
Vendor: deltacontrols					
Product: entelitouch_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-22	6.1	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 was discovered to contain a cross-site scripting (XSS) vulnerability via the Username parameter. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-29732**	https://www.deltacontrols.com/	O-DEL-ENTE-200622/1134
Cleartext Transmission of Sensitive Information	02-Jun-22	5.9	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 was discovered to transmit and store sensitive information in cleartext. This vulnerability allows attackers to intercept HTTP Cookie authentication credentials via a man-in-the-middle attack. **CVE ID : CVE-2022-29733**	https://www.deltacontrols.com/	O-DEL-ENTE-200622/1135
Cross-Site Request Forgery (CSRF)	02-Jun-22	8.8	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 allows	https://www.deltacontrols.com/	O-DEL-ENTE-200622/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary commands via a crafted HTTP request. **CVE ID : CVE-2022-29735**		
Vendor: Dlink					
Product: dir-890l_firmware					
N/A	03-Jun-22	8.8	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-890L 1.20b01 allows attackers to execute arbitrary code due to the hardcoded option Wake-On-Lan for the parameter 'descriptor' at SetVirtualServerSettings.php. **CVE ID : CVE-2022-29778**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--200622/1137
Out-of-bounds Write	02-Jun-22	9.8	The LAN-side Web-Configuration Interface has Stack-based Buffer Overflow vulnerability in the D-Link Wi-Fi router firmware DIR-890L DIR890LA1_FW107b09.bin and previous versions. The function created at 0x17958 of /htdocs/cgibin will call sprintf without checking the length of strings in parameters given by HTTP header and can be controlled by	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--200622/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users easily. The attackers can exploit the vulnerability to carry out arbitrary code by means of sending a specially constructed payload to port 49152. **CVE ID : CVE-2022-30521**		
Vendor: Fedoraproject					
Product: fedora					
Uncontrolled Resource Consumption	07-Jun-22	7.5	A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the Kube API. The ExecSync request runs commands in a container and logs the output of the command. This output is then read by CRI-O after command execution, and it is read in a manner where the entire file corresponding to the output of the command is read in. Thus, if the output of the command is large it is possible to exhaust the memory or the disk space of the node when CRI-O reads the output of the command. The highest threat from	https://github.com/cri-o/cri-o/commit/f032cf649ecc7e0c46718bd9e7814bfb317cb544	O-FED-FEDO-200622/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability is system availability. **CVE ID : CVE-2022-1708**		
NULL Pointer Dereference	02-Jun-22	6.8	With shadow paging enabled, the INVPCID instruction results in a call to kvm_mmu_invpcid_gva. If INVPCID is executed with CR0.PG=0, the invlpg callback is not set and the result is a NULL pointer dereference. **CVE ID : CVE-2022-1789**	https://bugzilla.redhat.com/show_bug.cgi?id=1832397	O-FED-FEDO-200622/1140
Incorrect Authorization	02-Jun-22	7.5	An access control bypass vulnerability found in 389-ds-base. That mishandling of the filter that would yield incorrect results, but as that has progressed, can be determined that it actually is an access control bypass. This may allow any remote unauthenticated user to issue a filter that allows searching for database items they do not have access to, including but not limited to potentially userPassword	https://bugzilla.redhat.com/show_bug.cgi?id=2091781	O-FED-FEDO-200622/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hashes and other sensitive data. **CVE ID : CVE-2022-1949**		
Vendor: Google					
Product: android					
Use After Free	06-Jun-22	8.8	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872. **CVE ID : CVE-2022-21745**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1142
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698;	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06479698. **CVE ID : CVE-2022-21746**		
Out-of-bounds Read	06-Jun-22	4.4	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078. **CVE ID : CVE-2022-21747**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1144
Incorrect Permission Assignment for Critical Resource	06-Jun-22	5.5	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030. **CVE ID : CVE-2022-21748**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1145
Incorrect Permission	06-Jun-22	5.5	In telephony, there is a possible	https://corp.mediatek.com/pro	O-GOO-ANDR-200622/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058. **CVE ID : CVE-2022-21749**	duct-security-bulletin/June-2022	
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521283; Issue ID: ALPS06521283. **CVE ID : CVE-2022-21750**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1147
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, 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/June-2022	O-GOO-ANDR-200622/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511132; Issue ID: ALPS06511132. **CVE ID : CVE-2022-21751**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873; Issue ID: ALPS06493873. **CVE ID : CVE-2022-21752**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1149
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06493873;	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06493899. **CVE ID : CVE-2022-21753**		
Out-of-bounds Write	06-Jun-22	6.7	In WLAN driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535953; Issue ID: ALPS06535953. **CVE ID : CVE-2022-21754**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1151
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06545464; Issue ID: ALPS06545464. **CVE ID : CVE-2022-21755**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-22	4.4	In WLAN 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: ALPS06535950; Issue ID: ALPS06535950. **CVE ID : CVE-2022-21756**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1153
Improper Validation of Integrity Check Value	06-Jun-22	7.5	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894. **CVE ID : CVE-2022-21757**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1154
Double Free	06-Jun-22	6.7	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600. **CVE ID : CVE-2022-21758**		
Out-of-bounds Write	06-Jun-22	6.7	In power service, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419106; Issue ID: ALPS06419077. **CVE ID : CVE-2022-21759**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1156
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479562; Issue ID: ALPS06479562.	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21760		
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479532; Issue ID: ALPS06479532. **CVE ID : CVE-2022-21761**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1158
Integer Overflow or Wraparound	06-Jun-22	4.4	In apusys driver, there is a possible system crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477946; Issue ID: ALPS06477946. **CVE ID : CVE-2022-21762**	https://corp.mediatek.com/product-security-bulletin/June-2022	O-GOO-ANDR-200622/1159
Use of Hard-coded Credentials	02-Jun-22	9.8	LinkPlay Sound Bar v1.0 allows attackers to escalate privileges via a hardcoded password for the SSL certificate.	N/A	O-GOO-ANDR-200622/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28605		
Exposure of Resource to Wrong Sphere	07-Jun-22	3.3	Sensitive information exposure in low-battery dumpstate log prior to SMR Jun-2022 Release 1 allows local attackers to get SIM card information. **CVE ID : CVE-2022-28794**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1161
Improper Input Validation	07-Jun-22	5.3	Improper input validation check logic vulnerability in SECRIL prior to SMR Jun-2022 Release 1 allows attackers to trigger crash. **CVE ID : CVE-2022-30709**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1162
Improper Input Validation	07-Jun-22	9.1	Improper validation vulnerability in RemoteViews prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-30710**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1163
Improper Input Validation	07-Jun-22	9.1	Improper validation vulnerability in FeedsInfo prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-30711**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Jun-22	9.1	Improper validation vulnerability in KfaOptions prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-30712**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1165
Improper Input Validation	07-Jun-22	9.1	Improper validation vulnerability in LSOItemData prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities. **CVE ID : CVE-2022-30713**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1166
Exposure of Resource to Wrong Sphere	07-Jun-22	3.3	Information exposure vulnerability in SemIWCMonitor prior to SMR Jun-2022 Release 1 allows local attackers to get MAC address information. **CVE ID : CVE-2022-30714**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1167
Missing Authorization	07-Jun-22	5.3	Improper access control vulnerability in DofViewer prior to SMR Jun-2022 Release 1 allows attackers to control floating system alert window. **CVE ID : CVE-2022-30715**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1168
Improper Handling	07-Jun-22	5.3	Unprotected broadcast in	https://security.samsungmobile	O-GOO-ANDR-200622/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Exceptional Conditions			sendIntentForToastDumpLog in DisplayToast prior to SMR Jun-2022 Release 1 allows untrusted applications to access toast message information from device. **CVE ID : CVE-2022-30716**	.com/securityUpdate.smsb?year=2022&month=6	
Incorrect Authorization	07-Jun-22	7.5	Improper caller check in AR Emoji prior to SMR Jun-2022 Release 1 allows untrusted applications to use some camera functions via deeplink. **CVE ID : CVE-2022-30717**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1170
Improper Input Validation	07-Jun-22	5.3	Improper input validation check logic vulnerability in libsmkvextractor prior to SMR Jun-2022 Release 1 allows attackers to trigger crash. **CVE ID : CVE-2022-30719**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1171
Improper Input Validation	07-Jun-22	5.3	Improper input validation check logic vulnerability in libsmkvextractor prior to SMR Jun-2022 Release 1 allows attackers to trigger crash.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30720		
Improper Input Validation	07-Jun-22	5.3	Improper input validation check logic vulnerability in libsmkvextractor prior to SMR Jun-2022 Release 1 allows attackers to trigger crash. **CVE ID : CVE-2022-30721**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1173
N/A	07-Jun-22	9.8	Implicit Intent hijacking vulnerability in Samsung Account prior to SMR Jun-2022 Release 1 allows attackers to bypass user confirmation of Samsung Account. **CVE ID : CVE-2022-30722**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1174
Improper Handling of Exceptional Conditions	07-Jun-22	4.3	Broadcasting Intent including the BluetoothDevice object without proper restriction of receivers in activateVoiceRecognitionWithDevice function of Bluetooth prior to SMR Jun-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-30723**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-Jun-22	4.3	Broadcasting Intent including the BluetoothDevice object without proper restriction of receivers in sendIntentSessionCompleted function of Bluetooth prior to SMR Jun-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-30724**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1176
Improper Handling of Exceptional Conditions	07-Jun-22	4.3	Broadcasting Intent including the BluetoothDevice object without proper restriction of receivers in sendIntentSessionError function of Bluetooth prior to SMR Jun-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-30725**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1177
N/A	07-Jun-22	7.8	Unprotected component vulnerability in DeviceSearchTrampoline in SecSettingsIntelligence prior to SMR Jun-2022 Release 1 allows local attackers to launch activities of	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SecSettingsIntelligence. **CVE ID : CVE-2022-30726**		
Improper Handling of Exceptional Conditions	07-Jun-22	5.5	Improper handling of insufficient permissions vulnerability in addAppPackageNameToAllowList in PersonaManagerService prior to SMR Jun-2022 Release 1 allows local attackers to set some setting value in work space. **CVE ID : CVE-2022-30727**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1179
Exposure of Resource to Wrong Sphere	07-Jun-22	3.3	Information exposure vulnerability in ScanPool prior to SMR Jun-2022 Release 1 allows local attackers to get MAC address information. **CVE ID : CVE-2022-30728**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1180
N/A	07-Jun-22	4.6	Implicit Intent hijacking vulnerability in Settings prior to SMR Jun-2022 Release 1 allows attackers to get Wi-Fi SSID and password via a malicious QR code scanner.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6	O-GOO-ANDR-200622/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30729		
Vendor: H3C					
Product: magic_r100_firmware					
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the CMD parameter at /goform/aspForm. **CVE ID : CVE-2022-30909**	N/A	O-H3C-MAGI-200622/1182
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the GO parameter at /goform/aspForm. **CVE ID : CVE-2022-30910**	N/A	O-H3C-MAGI-200622/1183
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateWanParams parameter at /goform/aspForm. **CVE ID : CVE-2022-30912**	N/A	O-H3C-MAGI-200622/1184
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the	N/A	O-H3C-MAGI-200622/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipqos_set_bandwidth parameter at /goform/aspForm. **CVE ID : CVE-2022-30913**		
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateMacClone parameter at /goform/aspForm. **CVE ID : CVE-2022-30914**	N/A	O-H3C-MAGI-200622/1186
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateSnat parameter at /goform/aspForm. **CVE ID : CVE-2022-30915**	N/A	O-H3C-MAGI-200622/1187
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTelnetDebug parameter at /goform/aspForm. **CVE ID : CVE-2022-30916**	N/A	O-H3C-MAGI-200622/1188
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to	N/A	O-H3C-MAGI-200622/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow vulnerability via the AddWlanMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30917**		
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTelnet parameter at /goform/aspForm. **CVE ID : CVE-2022-30918**	N/A	O-H3C-MAGI-200622/1190
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Edit_BasicSSID_5G parameter at /goform/aspForm. **CVE ID : CVE-2022-30919**	N/A	O-H3C-MAGI-200622/1191
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Edit_BasicSSID parameter at /goform/aspForm. **CVE ID : CVE-2022-30920**	N/A	O-H3C-MAGI-200622/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the SetMobileAPInfoById parameter at /goform/aspForm. **CVE ID : CVE-2022-30921**	N/A	O-H3C-MAGI-200622/1193
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the EditWlanMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30922**	N/A	O-H3C-MAGI-200622/1194
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTimingtime WifiAndLed parameter at /goform/aspForm. **CVE ID : CVE-2022-30923**	N/A	O-H3C-MAGI-200622/1195
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the SetAPWifiorLedInfo	N/A	O-H3C-MAGI-200622/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ById parameter at /goform/aspForm. **CVE ID : CVE-2022-30924**		
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the AddMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30925**	N/A	O-H3C-MAGI-200622/1197
Out-of-bounds Write	08-Jun-22	9.8	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the EditMacList parameter at /goform/aspForm. **CVE ID : CVE-2022-30926**	N/A	O-H3C-MAGI-200622/1198
Vendor: ict					
Product: protege_gx_firmware					
Use of Password Hash With Insufficient Computational Effort	02-Jun-22	4.3	An access control issue in ICT Protege GX/WX 2.08 allows attackers to leak SHA1 password hashes of other users. **CVE ID : CVE-2022-29731**	https://www.ict.co/	O-ICT-PROT-200622/1199
Product: protege_wx_firmware					
Use of Password	02-Jun-22	4.3	An access control issue in ICT Protege	https://www.ict.co/	O-ICT-PROT-200622/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Hash With Insufficient Computational Effort			GX/WX 2.08 allows attackers to leak SHA1 password hashes of other users. **CVE ID : CVE-2022-29731**		
Vendor: keysight					
Product: n6841a_rf_firmware					
Deserialization of Untrusted Data	02-Jun-22	9.8	The affected products are vulnerable of untrusted data due to deserialization without prior authorization/authentication, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2022-1660**	N/A	O-KEY-N684-200622/1201
Relative Path Traversal	02-Jun-22	7.5	The affected products are vulnerable to directory traversal, which may allow an attacker to obtain arbitrary operating system files. **CVE ID : CVE-2022-1661**	N/A	O-KEY-N684-200622/1202
Product: n6854a_firmware					
Deserialization of Untrusted Data	02-Jun-22	9.8	The affected products are vulnerable of untrusted data due to deserialization without prior authorization/authentication, which may	N/A	O-KEY-N685-200622/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2022-1660**		
Relative Path Traversal	02-Jun-22	7.5	The affected products are vulnerable to directory traversal, which may allow an attacker to obtain arbitrary operating system files. **CVE ID : CVE-2022-1661**	N/A	O-KEY-N685-200622/1204
Vendor: Linux					
Product: linux_kernel					
Use After Free	02-Jun-22	7.8	The root cause of this vulnerability is that the ioctl$DRM_IOCTL_MODE_DESTROY_DUMB can decrease refcount of *drm_vgem_gem_object *(created in *vgem_gem_dumb_create*) concurrently, and *vgem_gem_dumb_create *will access the freed drm_vgem_gem_object. **CVE ID : CVE-2022-1419**	N/A	O-LIN-LINU-200622/1205
Use After Free	02-Jun-22	7.8	Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a	N/A	O-LIN-LINU-200622/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system. **CVE ID : CVE-2022-1652**		
Use After Free	02-Jun-22	7.8	A use-after-free flaw was found in the Linux kernel's io_uring subsystem in the way a user sets up a ring with IORING_SETUP_IOPOLL with more than one task completing submissions on this ring. This flaw allows a local user to crash or escalate their privileges on the system. **CVE ID : CVE-2022-1786**	N/A	O-LIN-LINU-200622/1207
NULL Pointer Dereference	02-Jun-22	6.8	With shadow paging enabled, the INVPCID instruction results in a call to kvm_mmu_invpcid_gva. If INVPCID is executed with CR0.PG=0, the invlpg callback is not set and the result is a	https://bugzilla.redhat.com/show_bug.cgi?id=1832397	O-LIN-LINU-200622/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NULL pointer dereference. **CVE ID : CVE-2022-1789**		
Use After Free	02-Jun-22	7.8	net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free. **CVE ID : CVE-2022-32250**	https://www.openwall.com/lists/oss-security/2022/05/31/1, https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/net/netfilter?id=520778042ccca019f3ffa136dd0ca565c486cedd, http://www.openwall.com/lists/oss-security/2022/06/03/1	O-LIN-LINU-200622/1209
Observable Discrepancy	05-Jun-22	3.3	The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used. **CVE ID : CVE-2022-32296**	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4c2c8f03a5ab7cb04ec64724d7d176d00bcc91e5, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.9	O-LIN-LINU-200622/1210
Vendor: Microsoft					
Product: windows					
Improper Preservation of	02-Jun-22	7.8	eG Agent before 7.2 has weak file permissions that	N/A	O-MIC-WIND-200622/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			enable escalation of privileges to SYSTEM. **CVE ID : CVE-2022-29594**		
Product: windows_10					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1212
Product: windows_11					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1213
Product: windows_7					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1214
Product: windows_8.1					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1215
Product: windows_rt_8.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1216
Product: windows_server_2008					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1217
Product: windows_server_2012					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1218
Product: windows_server_2016					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1219
Product: windows_server_2019					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_server_2022					
N/A	01-Jun-22	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30190**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	O-MIC-WIND-200622/1221
Vendor: Netapp					
Product: hci_bootstrap_os					
Cleartext Transmission of Sensitive Information	02-Jun-22	4.3	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP step even when HTTP is provided in theURL. This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when it built the HSTS cache. Or the otherway around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL. **CVE ID : CVE-2022-30115**	https://security.netapp.com/advisory/ntap-20220609-0009/	O-NET-HCI_-200622/1222
Vendor: owllabs					
Product: meeting_owl_pro_firmware					
Exposure of Sensitive Information to an	02-Jun-22	6.5	Owl Labs Meeting Owl 5.2.0.15 allows attackers to retrieve the passcode hash	N/A	O-OWL-MEET-200622/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			via a certain c 10 value over Bluetooth. **CVE ID : CVE-2022-31459**		
Use of Hard-coded Credentials	02-Jun-22	7.4	Owl Labs Meeting Owl 5.2.0.15 allows attackers to activate Tethering Mode with hard-coded hoothoot credentials via a certain c 150 value. **CVE ID : CVE-2022-31460**	N/A	O-OWL-MEET-200622/1224
Improper Authentication	02-Jun-22	6.5	Owl Labs Meeting Owl 5.2.0.15 allows attackers to deactivate the passcode protection mechanism via a certain c 11 message. **CVE ID : CVE-2022-31461**	N/A	O-OWL-MEET-200622/1225
Use of Hard-coded Credentials	02-Jun-22	8.8	Owl Labs Meeting Owl 5.2.0.15 allows attackers to control the device via a backdoor password (derived from the serial number) that can be found in Bluetooth broadcast data. **CVE ID : CVE-2022-31462**	N/A	O-OWL-MEET-200622/1226
Improper Authentication	02-Jun-22	7.1	Owl Labs Meeting Owl 5.2.0.15 does not require a password for Bluetooth commands, because only client-side	N/A	O-OWL-MEET-200622/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication is used. **CVE ID : CVE-2022-31463**		
Vendor: Redhat					
Product: enterprise_linux					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jun-22	6.3	An out-of-bounds read flaw was found in the Linux kernel's TeleTYpe subsystem. The issue occurs in how a user triggers a race condition using ioctls TIOCSPTLCK and TIOCGPTPEER and TIOCSTI and TCXONC with leakage of memory in the flush_to_ldisc function. This flaw allows a local user to crash the system or read unauthorized random data from memory. **CVE ID : CVE-2022-1462**	N/A	O-RED-ENTE-200622/1228
Use After Free	02-Jun-22	7.8	Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a	N/A	O-RED-ENTE-200622/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service condition on the system. **CVE ID : CVE-2022-1652**		
Uncontrolled Resource Consumption	07-Jun-22	7.5	A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the Kube API. The ExecSync request runs commands in a container and logs the output of the command. This output is then read by CRI-O after command execution, and it is read in a manner where the entire file corresponding to the output of the command is read in. Thus, if the output of the command is large it is possible to exhaust the memory or the disk space of the node when CRI-O reads the output of the command. The highest threat from this vulnerability is system availability. **CVE ID : CVE-2022-1708**	https://github.com/cri-o/cri-o/commit/f032cf649ecc7e0c46718bd9e7814bfb317cb544	O-RED-ENTE-200622/1230
NULL Pointer	02-Jun-22	6.8	With shadow paging enabled, the INVPCID instruction	https://bugzilla.redhat.com/sh	O-RED-ENTE-200622/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			results in a call to kvm_mmu_invpcid_g va. If INVPCID is executed with CR0.PG=0, the invlpg callback is not set and the result is a NULL pointer dereference. **CVE ID : CVE-2022-1789**	ow_bug.cgi?id= 1832397	
Incorrect Authorizati on	02-Jun-22	7.5	An access control bypass vulnerability found in 389-ds-base. That mishandling of the filter that would yield incorrect results, but as that has progressed, can be determined that it actually is an access control bypass. This may allow any remote unauthenticated user to issue a filter that allows searching for database items they do not have access to, including but not limited to potentially userPassword hashes and other sensitive data. **CVE ID : CVE-2022-1949**	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 2091781	O-RED-ENTE-200622/1232
Vendor: Rockwellautomation					
Product: compactlogix_5370_firmware					
Uncontroll ed	02-Jun-22	8.6	A malformed Class 3 common industrial	https://www.ci sa.gov/uscert/ic	O-ROC-COMP-200622/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	s/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	
Product: compactlogix_5380_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	O-ROC-COMP-200622/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1797		
Product: compactlogix_5480_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	O-ROC-COMP-200622/1235
Product: compact_guardlogix_5370_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	O-ROC-COMP-200622/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**		
Product: compact_guardlogix_5380_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	O-ROC-COMP-200622/1237
Product: controllogix_5570_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answe	O-ROC-CONT-200622/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	r_view/a_id/1135559	
Product: controllogix_5580_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	O-ROC-CONT-200622/1239
Product: guardlogix_5570_firmware					
Uncontrolled Resource	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message	https://www.cisa.gov/uscert/ics/advisories/ics	O-ROC-GUAR-200622/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online. **CVE ID : CVE-2022-1797**	a-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	
Product: guardlogix_5580_firmware					
Uncontrolled Resource Consumption	02-Jun-22	8.6	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1135559	O-ROC-GUAR-200622/1241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1797		
Vendor: Schneider-electric					
Product: powerlogic_ion_setup_firmware					
Improper Input Validation	02-Jun-22	8.8	A CWE-20: Improper Input Validation vulnerability exists that could cause potential remote code execution when an attacker is able to intercept and modify a request on the same network or has configuration access to an ION device on the network. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30232**	https://www.se.com/ww/en/download/document/SEVD-2022-130-01/	O-SCH-POWE-200622/1242
Product: wiser_smart_eer21000_firmware					
Improper Input Validation	02-Jun-22	6.5	A CWE-20: Improper Input Validation vulnerability exists that could allow the product to be maliciously manipulated when the user is tricked into performing certain actions on a webpage. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30233		
Use of Hard-coded Credentials	02-Jun-22	9.8	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could allow arbitrary code to be executed when root level access is obtained. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30234**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1244
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow unauthorized access when an attacker uses brute force. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30235**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1245
Incorrect Resource Transfer Between Spheres	02-Jun-22	8.2	A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could allow unauthorized access when an attacker	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uses cross-domain attacks. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30236**		
Missing Encryption of Sensitive Data	02-Jun-22	7.5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow authentication credentials to be recovered when an attacker breaks the encoding. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30237**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1247
Improper Authentication	02-Jun-22	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow an attacker to take over the admin account when an attacker hijacks a session. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30238**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1248
Product: wiser_smart_eer21001_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Jun-22	6.5	A CWE-20: Improper Input Validation vulnerability exists that could allow the product to be maliciously manipulated when the user is tricked into performing certain actions on a webpage. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30233**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1249
Use of Hard-coded Credentials	02-Jun-22	9.8	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could allow arbitrary code to be executed when root level access is obtained. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30234**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1250
Improper Restriction of Excessive Authentication Attempts	02-Jun-22	9.8	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow unauthorized access when an attacker uses brute force. Affected Products:	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30235**		
Incorrect Resource Transfer Between Spheres	02-Jun-22	8.2	A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could allow unauthorized access when an attacker uses cross-domain attacks. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30236**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1252
Missing Encryption of Sensitive Data	02-Jun-22	7.5	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow authentication credentials to be recovered when an attacker breaks the encoding. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30237**	https://www.se.com/ww/en/download/document/SEVD-2022-130-03/	O-SCH-WISE-200622/1253
Improper Authentication	02-Jun-22	8.8	A CWE-287: Improper Authentication vulnerability exists	https://www.se.com/ww/en/download/docu	O-SCH-WISE-200622/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could allow an attacker to take over the admin account when an attacker hijacks a session. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior) **CVE ID : CVE-2022-30238**	ment/SEVD-2022-130-03/	
Vendor: Siemens					
Product: biograph_horizon_pet\/ct_systems_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2),	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-BIOG-200622/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: magnetom_numaris_x_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-MAGN-200622/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: mammomat_revelation_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-MAMM-200622/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the affected system if ports 32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: naeotom_alpha_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-NAEO-200622/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			32912/tcp or 32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.all_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			32914/tcp are reachable. **CVE ID : CVE-2022-29875**		
Product: somatom_go.now_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: somatom_go.open_pro_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: somatom_go.sim_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: somatom_go.up_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: somatom_x.cite_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: somatom_x.creed_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SOMA-200622/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_evo_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SYMB-200622/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_e_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SYMB-200622/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_intevo_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SYMB-200622/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_s_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SYMB-200622/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Product: symbia_t_firmware					
Deserialization of Untrusted Data	01-Jun-22	9.8	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions <	https://www.siemens-healthineers.com/support-documentation/cybersecurity/shsa-455016	O-SIE-SYMB-200622/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29875		
Vendor: Tenda					
Product: hg6_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Jun-22	8.8	Tenda Technology Co.,Ltd HG6 3.3.0-210926 was discovered to contain a command injection vulnerability via the pingAddr and traceAddr parameters. This vulnerability is exploited via a crafted POST request. **CVE ID : CVE-2022-30425**	https://www.tendacn.com/	O-TEN-HG6_-200622/1271
Vendor: tigera					
Product: calico_os					
Improper Input Validation	06-Jun-22	5.5	Clusters using Calico (version 3.22.1 and below), Calico Enterprise (version 3.12.0 and below), may be vulnerable to route hijacking with the floating IP feature. Due to insufficient validation, a privileged attacker may be able to set a floating IP annotation to a pod even if the feature is not enabled. This may allow the attacker to intercept and reroute traffic to	https://www.tigera.io/security-bulletins-tta-2022-001/	O-TIG-CALI-200622/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their compromised pod. **CVE ID : CVE-2022-28224**		
Vendor: usr					
Product: usr-g800v2_firmware					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	O-USR-USR--200622/1273
Product: usr-g806_firmware					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	O-USR-USR--200622/1274
Product: usr-g807_firmware					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded	https://www.pusr.com/	O-USR-USR--200622/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**		
Product: usr-g808_firmware					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	O-USR-USR--200622/1276
Product: usr-lg220-l_firmware					
Use of Hard-coded Credentials	02-Jun-22	9.8	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device. **CVE ID : CVE-2022-29730**	https://www.pusr.com/	O-USR-USR--200622/1277
Vendor: Verizon					
Product: 4g_lte_network_extender_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Jun-22	7.5	Verizon 4G LTE Network Extender GA4.38 - V0.4.038.2131 utilizes a weak default admin password generation algorithm which generates passwords that are accessible to unauthenticated attackers via the webUI login page. **CVE ID : CVE-2022-29729**	https://www.verizon.com/	O-VER-4G_L-200622/1278
Vendor: Watchguard					
Product: fireware					
N/A	07-Jun-22	9.1	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. **CVE ID : CVE-2022-25361**	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00004, https://watchguard.com	O-WAT-FIRE-200622/1279